UNIVERSIDAD DE EL SALVADOR

Facultad de Ciencias Económicas

Escuela de Contaduría Pública

MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

PARA EL PROCESAMIENTO ELECTRÓNICO DE DATOS CONTABLES

Trabajo de investigación presentado por:

ALFARO SALGADO, JOSUÉ DARÍO

LOZA LOPEZ, VANESSA JHANINA

MURCIA ALBERTO, GUADALUPE NOHEMY

Para Optar al Grado de:

LICENCIADO EN CONTADURIA PÚBLICA

Febrero de 2009

San Salvador, El Salvador, Centro América

UNIVERSIDAD DE EL SALVADOR
AUTORIDADES UNIVERSITARIAS

Rector	: Msc. Rufino Antonio Quezada Sánchez
Secretario General	: Msc. Douglas Vladimir Alfaro Chávez
Decano de la Facultad de Ciencias Económicas	: Msc. Roger Armando Arias Alvarado
Secretaria de la Facultad de Ciencias Económicas	: M.A.E. José Ciriaco Gutiérrez Contreras
Director Seminario de Graduación	: Lic. Roberto Carlos Jovel Jovel
Asesor	: Lic. Mario Hernán Cornejo Pérez
Docente Director	: Lic. Mario Hernán Cornejo Pérez
Docente Coordinador	: Licda. Elsy Guadalupe Monge Vaquerano

Febrero de 2009

San Salvador, El Salvador, Centro América

INDICE

CAPITULO II

CAPITULO III

DEDICATORIA

El presente trabajo de graduación esta dedicado a Dios todo poderoso, por habernos dado fuerza, vida y sabiduría para desarrollar la investigación y permitirnos culminar esta importante etapa en nuestras vidas.

A nuestros padres por habernos brindado todo su amor y paciencia durante cada etapa de nuestra vida y su apoyo incondicional en este ultimo paso, que es el presente trabajo de graduación.

A nuestros familiares que nos han brindado todo su afecto y cariño y han permanecido a nuestro lado animándonos a seguir siempre hacia adelante

A nuestro asesor de tesis, Lic. Mario Hernán Cornejo por habernos ayudado en este importante proceso, por apoyarnos de la manera más profesional para que esta investigación se realizara.

A nuestros amigos, por su apoyo a lo largo de esta trayectoria y de este proceso, ya que siempre nos brindaron su ayuda en forma oportuna y desinteresada.

A todos ustedes nuestros más sinceros agradecimientos.

AGRADECIMIENTOS.

Al Creador de los cielos y la tierra y salvador de mi vida Jesucristo, le dedico este triunfo académico, porque sin el nada de esto seria posible, a mis padres Marcos Murcia y Ana Julia Alberto por todo su apoyo y cariño, gracias por los sacrificios realizados en formar mi carácter, a mis hermanos y familiares por sus oraciones, a Jesús Guzmán por cada minuto de su tiempo dedicado en apoyarme, amarme y brindarme su confianza, a todos mis amig@s que siempre permanecieron a mi lado, y muy especialmente a Vanesa Loza, Darío Alfaro, Gabriel Valladares y Silvia Panameño, por ser parte de mi familia y estar siempre presentes en mi corazón.

"Hubiera yo desmayado, sino creyese que veré la bondad de Jehová" Salmo 27: 13

Guadalupe Nohemy Murcia Alberto

Agradezco primeramente a Diosito todo poderoso por haberme dado la vida, las fuerzas y las perseverancia para llegar hasta aquí y haber alcanzado este titulo, a nuestra madre La Virgen María por siempre interceder antes Dios y yo se que ella ha estado rogando a nuestro Padre Celestial para que llegue a obtener este titulo. A mis padres Ana Delmy Salgado y José María Alfaro por que siempre me han apoyado y me siguen apoyando, ya que con su ayuda he podido culminar esta etapa en mi vida; a mis hermanos Manuel Alejandro Alfaro y Delmy Margarita Alfaro por haberme brindado su ayuda cuando lo necesite y estar siempre a mi lado, a mi tía Margarita y mi tío Arístides por darme su apoyo y todo su cariño, ya que los considero casi como mis segundos padres; a

mis dos compañeras de tesis, Vanessa Loza mi novia y a Guadalupe Murcia que más que ser compañera es mi mas grande amiga, por aguantarme a lo largo de esta carrera y más importante en este proceso, creo que Dios no me pudo mandar mejores compañeras para realizar este trabajo; al Lic. Mario Hernán Cornejo por darnos su ayuda tan profesional para realizar este trabajo; y por último a mis amig@s que me han acompañado a lo largo de esta carrera.

Josué Darío Alfaro Salgado.

Este es un logro para cada uno de nosotros, por lo quiero compartir con mi familia, amigos y conocidos, pero primeramente a Dios todo poderoso, por permitirme cumplir esta meta, por brindarme la vida, sabiduría, paciencia necesaria para no caer durante el camino, a mis queridos padres: Victorino Loza González y Concepción de Loza, por su apoyo incondicional en los buenos y malos momentos, a mis hermanos: Víctor Francisco Loza y Jonathan Ulises Loza, por su apoyo y paciencia durante todo este tiempo.

A mi querido amigo, compañero y novio Josué Darío Alfaro, por su amor, por sus consejos, por su paciencia, además por todo su apoyo en cada momento, a mi querida amiga Guadalupe Murcia por su paciencia, consejos, apoyo en los momentos difíciles y en los momentos de alegría, a sido mi mejor grupo de trabajo, y para finalizar a cada uno de mis amigos gracias por su apoyo, por sus consejos brindados.

Vanessa Jhanina Loza López.

RESUMEN EJECUTIVO

En la actualidad el creciente desarrollo del entorno globalizado que nos rodea, ha provocado que las organizaciones dinamicen las actividades que ejecutan, es con ello que la mayoría de empresas han experimentado una necesidad del uso de recursos informáticos para el procesamiento de la información contable, ya que la misma constituye uno de los insumos mas importantes que como contadores ofrecemos en nuestro que hacer diario, y se plasma como resultado final en los estados financieros.

Pero el surgimiento de nuevas tecnologías con lleva también el incremento de riesgos y amenazas a la información, es con dicha finalidad que el presente documento proporciona un manual de políticas de seguridad informática el cual persigue disminuir el riesgo de manipulación de la información contable al procesar electrónicamente la misma, el alcance de ellas se encuentra orientado en tres niveles considerados primordiales los cuales son la seguridad física, lógica y de redes.

Con base a lo anterior se realizo un estudio en las pequeñas y medianas empresas del sector comercio del municipio de San Salvador, registradas en la Cámara de Comercio e Industria de El Salvador; y el listados de las empresas del área metropolitana

proporcionado mediante el directorio de establecimientos de la Dirección General de Estadísticas y Censos, mediante el uso de la técnica del cuestionario y entrevistas fue posible comprobar que dichas empresas no hacen uso de políticas de seguridad informática para procesar la información contable, lo cual incrementa los riesgos de manipulación de la misma ya sea en forma interna o externa.

La presente investigación permitió determinar las conclusiones y recomendaciones siguientes:

Dentro de las empresas comerciales no poseen políticas de seguridad informática para el procesamiento electrónico de datos contables, que minimice el riesgo de manipulación de la información contable.

Por lo tanto se sugiere el uso de herramientas que le proporcionen los lineamientos adecuados tales como el presente documento.

INTRODUCCION

El procesamiento electrónico de datos, se ha convertido en una necesidad, en especial en el área contable, al manipular elevados volúmenes de información en forma confiable y oportuna, ello aunado a la importancia de conservar en forma íntegra, el resultado de los datos obtenidos para su posterior uso e interpretación para la toma de decisiones de la alta gerencia.

En EL Salvador, en su mayoría las empresas hacen uso de computadoras para el registro de las transacciones económicas, ya sea por medio de programas utilitarios (como Microsoft Word o Excel),y programas comerciales o diseñados a la medida, no obstante por ser un país en vías de desarrollo no se ha implementado una cultura de prevención de riesgos, por tal razón no se poseen políticas de seguridad informática para el procesamiento electrónico de datos contables, lo cual contribuye a incrementar el riesgo de manipulación de la información.

El trabajo de investigación que se presenta a continuación está orientado a proporcionar un manual de políticas para el procesamiento electrónico de datos contables, con base a normativas técnicas vigentes actualmente.

Dicho trabajo está dividido en cuatro capítulos que a continuación se describen:

El Capítulo I Marco Teórico, contiene los antecedentes, conceptualización y características de cada una de las variables que componen el tema de estudio, que son las generalidades con respecto a lo que es información contable, procesamiento electrónico de datos y seguridad informática.

El capítulo II trata sobre la metodología utilizada en la realización de la investigación, determinando desde la población hasta el análisis de los resultados; el tipo de estudio, la forma como se determinó la muestra, las unidades objeto de estudio y las técnicas e instrumentos utilizados; incluyendo un diagnóstico de los entornos encontrados, el cual describe el contexto actual del conocimiento de los contadores, las personas que procesan la información contable y los usuarios, con respecto al conocimiento de medidas de seguridad informática.

El capítulo III del documento es un manual de políticas de seguridad informática para el procesamiento electrónico de datos contables, el cual consta de una breve introducción al manual,

los objetivos que se persiguen, las políticas en si y las pautas que los usuarios deben tomar para su implementación y su monitoreo.

En el último capítulo se presentan las conclusiones y recomendaciones producto de la investigación y que puedan ser consideradas por los contadores públicos, los gremios de contadores, las empresas objetos de estudio y las instituciones gubernamentales correspondientes.

CAPITULO I

MARCO TEÓRICO

1.1. Información contable

La información contable constituye uno de los insumos más importantes que los contadores, ofrecen cotidianamente y este se plasma como resultado final en los estados financieros, los cuales llevan como objetivo primordial, servir a usuarios internos o externos a la entidad, la misma debe ser preparada conforme a normas y estándares regionales o internacionales.

En El Salvador con la finalidad de armonizar la normativa técnica aplicable en el país, en mes julio de 1996 el Colegio de Contadores Públicos Académicos, coordino revisión de 18 Normas de Contabilidad Financiera (NCF) vigentes a la fecha, como un punto a tratar en el marco del desarrollo de la IV Convención Nacional de Contadores, patrocinada por la Asociación de Contadores Públicos de El Salvador, el Colegio de Contadores Públicos Académicos de El Salvador, y la Corporación de Contadores de El Salvador; bajo el Lema **"La armonización contable y unidad gremial: Un reto imperativo ante la globalización"**, en la cual se revisaron las 18 NCF, y además se adicionan 10 más (de la 19 a la 28); procediendo a su legitimación de acuerdo con las conclusiones generales de la

Convención. A partir de entonces se conocen las 28 NCF, que no contaban con un respaldo legal solo el apoyo por parte del gremio.

La complejidad de los mercados, y los constantes cambios y modalidades de participar en la actividad económica, bajo un esquema de globalización e internacionalización de las economías; y el surgimiento de nuevos elementos que guían el reconocimiento, medición y revelación de las partidas en los estados financieros, fueron el indicador de las limitaciones técnicas contenidas en la normativa nacional.

Conscientes de dicha situación, el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditoría, con fecha 2 de septiembre de 1999, acordó que en la preparación de los estados financieros se implementarán Normas Internacionales de Contabilidad emitidas por el Comité de Normas Internacionales de Contabilidad (IASC) además de las regulaciones establecidas por el Consejo. Sin embargo, aún se encontraban vigentes las disposiciones del Código de Comercio, que en sus artículos 443 y 444 establecía la conformación de las partidas de los estados financieros, y las bases de estimación y valoración; lo cual dio surgimiento de discrepancias de las normas contables con la ley, lo cual representó para empresarios y contadores, una

verdadera polémica al momento de preparar los estados financieros, los cuales tenían que responder a las demandas de información de los inversionistas y demás usuarios de la información, así como a los requerimientos establecidos en las leyes mercantiles.

Desde el año 2000 El Salvador se encuentra en un proceso de adopción de las NIIF, lo cual genero cambios en la normativa legal y técnica aplicable hasta esa fecha, el 1 de abril de 2000, entro en vigencia las nuevas disposiciones contenidas en los artículos 443 y 444 del Código de Comercio y las nuevas atribuciones del Consejo de Vigilancia contenidas en la Ley Reguladora del Ejercicio de la Contaduría, con que se inicia la armonización de la infraestructura legal en materia mercantil, con la normativa técnica contable.

Con estas nuevas atribuciones y facultades, el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría, el día 5 de diciembre de 2000 acordó, que Las Normas Internacionales de Contabilidad se utilizarían como base general en la preparación y presentación de los estados financieros de las diferentes entidades siendo en forma obligatoria a partir del 1 de enero de 2002.

Pese a los constantes y diversos eventos de divulgación y capacitación desarrollados por el gremio profesional, el Consejo de Vigilancia, y otras instituciones dedicadas a la capacitación; no se logró una cobertura aceptable en el sector profesional ni en el sector empresarial. Ante esta situación el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría, emite acuerdo de fecha 1 de enero de 2002 para postergar la aplicación obligatoria de las normas y brinda parámetros adicionales a considerar.

En el Octubre del año de 2003 se adoptan en el país las Nuevas Normas Internacionales de Información Financiera NIIF (NIIF/ES para El Salvador), publicandose en D.O.06/01/04, que incluye las series de:

- Normas Internacionales de Contabilidad (NIC´s)
- Interpretaciones del Comité de Normas Internacionales de Contabilidad (SIC´s)
- Normas de Internacionales de Información Financiera No. 1 (NIIF 1)

En la actualidad, se ha desarrollado una normativa técnica internacional orientada únicamente a las pequeñas y medianas empresas denominada NIIF para PYMES, bajo esta ultima normativa las NIIF Full (Versión Completa de las NIIF) únicamente es

aplicable a las empresas listadas (que cotizan en bolsa de Valores) y se reconoce como no listadas a las PYMES, en el país aun no han entrado en vigencia.

1.1.1. Características de la información contable

"Comprensibilidad: Una cualidad esencial de la información suministrada en los estados financieros, es que la misma sea fácilmente entendible por los usuarios. Para este propósito se supone que ellos, tienen un conocimiento razonable de las actividades económicas y contables de la entidad. No obstante no se excluirá de los estados financieros, la información compleja que por su relevancia de cara a las necesidades de información, sea de difícil asimilación para ciertos personas.

Relevancia: Para ser útil, la información debe ser importante y ejercer influencia sobre las decisiones económicas de los que la utilizan, ayudándoles a evaluar sucesos pasados, presentes o futuros.

Representación Fiel: Para ser íntegra, la información debe representar las transacciones y sucesos acontecidos en la entidad, o que se puedan esperar razonablemente se presenten, por ejemplo un balance debe representar verdaderamente las transacciones sucesos que han dado como resultado los activos,

pasivos y patrimonio neto de la entidad en la fecha de la información, siempre que los mismos cumplan los requisitos para su reconocimiento.

Comparabilidad: Los usuarios deben ser capaces de cotejar los estados financieros de una entidad a lo largo del tiempo, con el fin de identificar las tendencias de la situación financiera y del desempeño, considerando que ellos desean comparar la situación financiera, el desempeño y flujos de fondos a lo largo del tiempo, es importante que los estados financieros muestren la información correspondiente a los periodos precedentes."[1]. Además deben elaborarse de tal forma que se puedan comparar con los estados financieros de entidades diferentes, evaluando su posición, desempeño y cambios en términos relativos.

1.1.2.Importancia de la información contable

Este tipo de información se divide en dos grandes ramas: la contabilidad externa y la contabilidad interna; la externa nos muestra la información que la empresa facilita al público en general siendo los principales usuarios de la misma los siguientes:

[1] Marco Conceptual para la Preparación y Presentación de los Estados Financieros, elaborado por IASB año 2001

a) Inversionistas: Se interesan principalmente por el reembolso de la suma invertida y el pago oportuno de sus rendimientos, brindando importancia a la capacidad futura de las empresas.
b) Empleados: El pago de sueldos y salarios proviene de los ingresos de las empresas. Por esta razón se interesan en saber si la empresa tiene la capacidad de pagarles en el corto y largo plazo.
c) Prestamistas: Se interesan en la capacidad de la empresa para poder pagar sus pasivos en el momento en que venzan.
d) Proveedores y Acreedores Comerciales: Esperan que la empresa tenga la capacidad de pagarles sus deudas, las cuales generalmente son a corto plazo.
e) Gobierno: Principal el gobierno busca en los estados financieros que las empresas, paguen los impuestos correspondientes a las utilidades y otras obligaciones tributarias a que sean objeto.
f) Público en General: El interés del público se atribuye a diferentes causas, por ejemplo las empresas hacen un aporte a su economía y en la mayoría de ocasiones su desaparición provoca trastornos en la misma.

La contabilidad interna, por su parte, tiene como objetivo brindar información sobre la posición financiera, resultados de

operación, cambios en la posición financiera de una empresa a los usuarios que necesitan de esta información para la toma de decisiones.a la vez suministra la información a los diferentes departamentos, para que trabajen correctamente.

1.1.3. Proceso de la información contable

La información contable, en un proceso lógico y secuencial al interior de una entidad, el cual incluye los siguientes elementos detallados a continuación:

a) Registrar
b) Cuantificar
c) Analizar
d) Interpretar

a) Registrar

En un sistema contable se deben registrar en forma sistemática y cronológica las transacciones derivadas de la actividad comercial en términos económicos. Previo a su registro, es necesario que la misma pueda ser clasificada conforme a la función o área de la que fue obtenida. Un registro completo de todas las actividades comerciales implica un gran volumen de información, demasiado extenso y diverso para que pueda ser útil en la toma de decisiones. Por lo tanto, la información se debe

clasificar en grupos o categorías; un ejemplo de ello es en el área de ingresos en la que se utilizan de soporte documentos como: facturas, comprobantes, recibos, notas, documentos mercantiles, etc. Siendo los mismos específicos para cada área de la entidad.

b) Cuantificar

La contabilidad es considerada como una técnica y no como una ciencia, ya que no puede ser exacta, debido a la necesidad de hacer uso de estimaciones contables que dependen en gran medida del juicio del contador u auditor.

Por ello es necesario resaltar que al referirse al termino cuantificación no se atribuya únicamente a la información expresada en términos numéricos, o que se encuentre consignado en un monto o valor de un documento, sino mas bien a la aplicabilidad de la técnica contable, y el análisis del impacto en los estados financieros, sobre la incorporación de una estimación o aplicación, en la que no se puede establecer con exactitud un valor, pero que su omisión incide en la presentación razonables de la información financiera de la entidad.

c) Analizar

La información contable proporciona a la entidad un insumo necesario para la toma de decisiones, por ejemplo los datos del área de ingresos brindan una apreciación del desempeño de la entidad en un periodo determinado y las oportunidades y fortalezas que posee en cada rubro que conforman dicha cuenta.

d) Interpretar

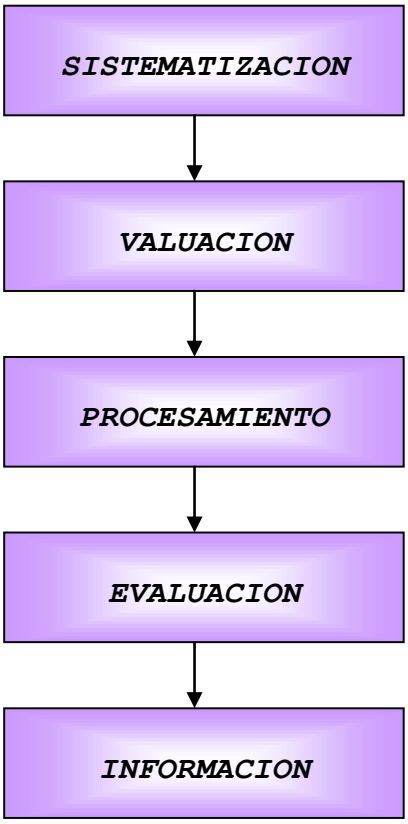
La utilidad de la información contable, implica un interés primordial para diferentes usuarios, ya sea a nivel interno o externo, ello se determina en virtud de hacia quienes va dirigida. Por ejemplo para la administración de una entidad la interpretación, de la misma es útil para futuras tomas de decisiones, pero para una institución financiera su apreciación se orientara a la capacidad de pago de la empresa, y la posibilidad de recuperar su inversión en ella.

Es por ello que la interpretación de la información contable sirve a un diverso número de usuarios, los cuales hacen uso de la misma para conocer sobre la entidad, su posicionamiento, solidez y administración a un periodo de tiempo determinado.

1.1.4. Fases del proceso contable computarizado

En el ámbito actual, las etapas para procesar la información contable se encuentran facilitadas por el uso de un sistema computarizado para el registro de las mismas, como se puede apreciar en el cuadro 1.

CUADRO N° 1: "FASES DEL PROCESO CONTABLE COMPUTARIZADO"



a) Sistematización

Este término es atribuible a la acción de implementar un sistema, lo cual en el ámbito contable se considera como el conjunto de procedimientos que se utilizan en el registro de las operaciones de una entidad, lo cual involucra el desarrollo, selección de sistemas de registros y control interno al interior de la organización.

Los sistemas contables poseen procedimientos, reglas, principios, cuentas, etc., debidamente estructurados y relacionados entre si, lo que hace posible realizar las operaciones con eficiencia, eficacia y economía.

b) Valuación:

Se cuantifica por medio de valores monetarios las operaciones, las que se deben encontrar debidamente documentadas y autorizadas.

c) Procesamiento:

La información contable se captura, clasifica, registra y calcula, con el objetivo que cada operación constituya un insumo que permita la obtención de informes, auxiliares y reportes necesarios para la elaboración de los estados financieros.

d) Evaluación:

En esta fase se analizan e interpretan los datos contenidos en los informes luego de su procesamiento y elaboración de los estados financieros.

e) Información:

La información obtenida se envía a la gerencia para la toma de decisiones de la entidad y la valorización de la situación actual y futura de la misma, por medio de proyecciones financieras a corto y largo plazo.

1.1.5.Normativa legal y técnica

1.1.5.1. Normativa legal

La información Contable en el ámbito jurídico tiene un alto grado de importancia por tal razón se establecieron lineamientos en relación al uso, importancia, y forma de presentación. En El Salvador con los cambios adoptados en la normativa técnica contable en el año 2000, tuvo un impacto de relevancia en las leyes vigentes a esa fecha, entre las cuales se pueden mencionar las siguientes:

a) Código de Comercio

En el mismo se establece en el Art. 411 los deberes de los comerciantes entre los cuales se puede mencionar, el llevar la contabilidad conforme los lineamientos que el presente Código establece. Por ello en el titulo III el legislador proporciona un apartado especial para la misma.

En el Art. 435 obliga a que el comerciante lleve la contabilidad en una forma organizada y de acuerdo con alguno de los sistemas generalmente aceptados en la materia y aprobados por quienes ejercen la función pública de auditoría, además hace mención de los registros que debe de poseer, no restringiendo la utilización de otros adicionales que sean necesarios por exigencias legales o contables.

En los Art. 436 al 437 se establece que el idioma de los registros contables será castellano y conforme a la moneda de curso legal; la cual es el colon salvadoreño y de acuerdo a la Ley de Integración Monetaria en Vigencia a partir del año 2001 también el dólar de los Estados Unidos de América.

A la fecha de dichas reformas se había determinado un monto de ¢100,000.00 colones para que los comerciantes se encontraran

obligados a llevar contabilidad formal; hecho que con las reformas del 12 de Junio de 2008 el limite se fija en $12,000.00 o ¢105,000.00 colones salvadoreños.

En los Arts 443, 444, 448 se especifica la importancia de la información contable dado que su utilidad a las instituciones gubernamentales es primordial por ello especifica que el balance general deberá expresar con veracidad y exactitud la situación financiera del negocio los cuales se elaboraran conforme a criterios emitidos por el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditoria (CVPCPA) o por Normas Internacionales de Contabilidad; ello implica aspectos como la expresión de los bienes y obligaciones que posee la entidad, las estimaciones realizadas conforme a lineamientos contables emitidos por el CVPCPA o la normativa internacional en su defecto.

b) Código Tributario

La importancia que la información contable proporciona a los usuarios externos es importante y por ello el marco jurídico tributario regula el uso y registro de la misma, logrando unificar y centralizar que los datos proporcionados al gobierno sean los mismos que son reflejados a las instituciones financieras entre otros organismos, según lo

establece en el Art.120 – A. Que las organizaciones del sector financiero como bancos, asociaciones cooperativas de ahorro y crédito, intermediarios financieros no bancarios, y cualquier otra entidad financiera, pública o privada, deben exigir a sus clientes o usuarios obligados a llevar contabilidad, el balance general y estado de resultados auditados para concederle financiamiento, cuando los montos superen los $ 40,000.00 los cuales corresponderán al ejercicio o periodo impositivo anterior a la solicitud de concesión de financiamiento. Además se auto facultan en el Art.126 para obligar a los contribuyentes a que proporcionen a la Administración Tributaria la contabilidad para examinarla y determinar si el reflejo de la misma es conforme a los montos declarados de impuesto o si existen inconsistencias. Para lo cual ha establecido mecanismos de control para las sociedades que cumplan los requisitos contenidos en el Art. 131 CT, siendo así que las mismas se dictaminen fiscalmente, con lo cual persigue determinar el cumplimiento de los contribuyentes fiscalmente y hacen uso de los registros contables y sus auxiliares para dicho fin.

En el literal c). Del Art. 135 se establece que se debe reflejar en el Dictamen y en el Informe Fiscal la realidad financiera y la situación tributaria, de conformidad a los

principios de contabilidad que establezca el CVPCPA y las leyes tributarias, respectivamente.

Además el legislador concede en la sección octava del Código, un apartado exclusivo de la obligación de llevar contabilidad formal, registros, inventarios y métodos de valuación de los mismos. Especificando que la contabilidad y su forma de registro, deben atender los lineamientos establecidos en el Código de Comercio, en tanto los mismos posean la documentación soporte, de su origen y se encuentren conforme los requerimientos tributarios señalados, los inventarios y sus métodos de valuación serán conforme la normativa técnica contable, y especifica que los tipos de inventario que los contribuyentes pueden adoptar son periódico o permanente. Los métodos de valuación aplicables fiscalmente dejan en desuso legal el método UEPS ya que no proporciona beneficios fiscales.

En el capítulo II fiscalizaciones en la sección primera Art. 173 establece que dentro de las facultades de la Administración Tributaria se encuentra que puede requerir de los contribuyentes tanto la información contable como cualquier tipo de registro, auxiliar que le garantice el cumplimiento del interés fiscal por lo cual la misma

legislación establece en sus artículos finales una gama de situaciones en las cuales la contabilidad puede proporcionar indicios de haber sido mal utilizada por el contribuyente y las sanciones a que puede ser objeto por ello

c) Ley de Impuesto Sobre la Renta

De acuerdo a la Ley de Impuesto Sobre la renta se reconoce en el Art.25 que la información contable es un insumo necesario en la distribución de las utilidades de los socios o accionistas pues representan el importe gravable de las rentas obtenidas en un periodo determinado.

El uso de la información contable es necesario como mecanismo de control en la aplicación de las leyes tributarias, en el Art. 30 se establece que es necesario en los contribuyentes obligados a llevar contabilidad formal calculen y registren la depreciación, adecuadamente ya que en el interés fiscal denota como medio de prueba la contabilidad en el cálculo de la misma, así como contribuye a respaldar la deducibilidad de los gastos necesarios para la fuente generadoras de rentas gravables realizadas por el contribuyente.

d) Ley de Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios

La información es una herramienta esencial para el pleno cumplimiento de las obligaciones formales y sustantivas, es por ello que en la Ley de Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios (IVA), la información contable forma parte importante en la deducibilidad del crédito fiscal generado en las operaciones del giro de la entidad, por lo que en el Art. 65 Párrafo tercero se estipula que los documentos expresados en la presente ley deberán además de cumplir los lineamientos de registros en libros auxiliares, encontrarse registrados en la contabilidad formal si fuere el caso ello en cumplimiento al Art. 141 CT.

La información desde el marco de regulación jurídico - legal suministra un valioso aporte para el cumplimiento de lineamientos establecidos por el estado para resguardar el interés del estado por medio de los impuestos, además de regular la información que es entregada a usuarios externos a la entidad. Respaldando el uso e interpretación que se haga de la misma.

1.1.5.2. Normativa técnica

En el año de 1973 nace el Comité de Normas Internacionales de Contabilidad (IASC), como resultado de un acuerdo tomado por ciertos organismos a nivel mundial (Alemania, Australia, Canadá, Estados Unidos, Francia, Holanda, Japón, México, Irlanda e Inglaterra).

Con base en la constitución de este organismo, se estableció un esquema normativo a nivel internacional llamado "Normas Internacionales de Contabilidad" (NIC), el cual se conformó de los siguientes pronunciamientos:

1) Normas Internacionales de Contabilidad, NIC (International Accounting Standards IAS), emitidas por el Comité de Normas Internacionales de Contabilidad (International Accounting Standards Comittee, IASC)

2) Interpretaciones de las Normas Internacionales de Contabilidad, emitidas por el Comité de Interpretaciones de IASC (Standing Intterpretations Commitée, SIC).

En El Salvador algunos de los esfuerzos de la profesión, orientados a la armonización de la normativa contable han sido los siguientes:

Hasta julio de 1996 el entonces Colegio de Contadores Públicos Académicos había coordinado la emisión de 18 Normas de Contabilidad Financiera (NCF).

A partir de julio de 1996 en el marco del desarrollo de la IV Convención Nacional de Contadores, se someten a revisión las 18 NCF, y se adicionan 10 más (de la 19 a la 28); procediendo a su legitimación. A partir de entonces se conocen las 28 NCF, que no contaban con un respaldo legal, sino únicamente del gremio.

La complejidad de los mercados, y los constantes cambios y modalidades de participar en la actividad económica, ahora bajo un esquema de globalización e internacionalización de las economías; y el surgimiento de nuevos elementos que guían el reconocimiento, medición y revelación de las partidas en los estados financieros, han sido el mejor indicador de las limitaciones técnicas contenidas en la normativa nacional.

Conscientes de tal situación, el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditoría, con fecha 2 de septiembre de 1999, tomó acuerdo, que en su segundo párrafo literalmente dice:

"II- En la preparación de los estados financieros deberán usarse Normas Internacionales de Contabilidad dictadas por el Comité de normas internacionales de Contabilidad (IASC) y/o aquellas regulaciones establecidas por este Consejo."

El 1 de abril de 2000, entran en vigencia las nuevas disposiciones contenidas en los artículos 443 y 444 del Código de Comercio y las atribuciones del Consejo de Vigilancia. Con estas nuevas atribuciones y facultades, el día 5 de diciembre de 2000 se toma el acuerdo de que las Normas Internacionales de Contabilidad se adoptaran como base en la preparación y presentación de los estados financieros en forma obligatoria a partir del 1 de enero del año 2002; creándose con ello la primera exigencia que integra aspectos técnicos y aspectos legales de materia mercantil.

Pese a los constantes y diversos eventos de divulgación y capacitación desarrollados por el gremio profesional, el Consejo de Vigilancia, y otras instituciones dedicadas a la capacitación; no se logró una cobertura aceptable en el sector profesional ni en el sector empresarial. Ante esta situación el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría, emite acuerdo de fecha 1 de enero de 2002, en el cual amplía el plazo de obligatoriedad para la entrada en vigencia de

las Normas Internacionales de Contabilidad, hasta el ejercicio económico que comienza el 1 de enero de 2004; estableciendo requisitos de divulgación en los estados financieros correspondientes al cierre de los ejercicios 2002 y 2003, se les solicitó a las empresas que mostraran las diferencias existentes entre las prácticas de contabilidad de ese momento y las Normas Internacionales de Contabilidad, incluyendo su cuantificación.

En noviembre de 2002, y dada la atribución de promover la educación continuada de los Contadores Públicos, el Consejo llevó a cabo el "Congreso de Contadores", con el lema "Las NIC`s, su análisis y aplicación en El Salvador".

En el 2002 se reconstituyó el antiguo Comité de Interpretaciones (SIC), con la nueva denominación de Comité de Interpretaciones de las Normas Internacionales de Información Financiera (CINIIF).

Al comenzar su trabajo, el IASB decidió que todas las Normas e Interpretaciones emitidas por el organismo predecesor continuarían siendo de aplicación a menos, y hasta el momento en que, fueran retiradas.

Debido a las constantes revisiones a las que han sido sometidas las Normas Internacionales de Contabilidad en los últimos años, se dificultó su adopción de una manera plena y sin reservas, ya que la afirmación "los estados financieros están preparados de acuerdo con las Normas Internacionales de Contabilidad", requiere de una aplicación total y sin reservas que incluya hasta las más recientes puestas en vigencia por el IASB; lo que creó confusión en las empresas al conocer una versión distinta cada año.

En El Salvador se adopto la Serie de Normas Internacionales de Información Financiera NIIF del año 2003 (NIIF/ES para El Salvador) que incluye la serie de:

- Normas Internacionales de Contabilidad (NIC´s)
- Interpretaciones del Comité de Normas Internacionales de Contabilidad (SIC´s)
- Normas de Internacionales de Información Financiera No. 1 (NIIF 1)

Las NIC que deben tomarse en cuenta para la adopción de las NIF/ES son las existentes al 31 de octubre de 2003, ya que el Consejo consideró conveniente hacer un corte cronológico para su adopción por primera vez, estableciendo que para la adopción de

las (NIF / ES) se tomarían en cuenta las NIC existentes a esa fecha.

Norma Internacional de Información Financiera para pequeñas y medianas entidades

En el año 2007, El Consejo de Normas Internacionales de Contabilidad invito a comentar sobre la propuesta de Proyecto de Norma Internacional de Información Financiera para Pequeñas y Medianas Entidades conocidas como NIIF para PYME, surgiendo como un material para ser comentado y en base a los diferentes aportes emitir un documento que presentara una base técnica aplicable a dichos sectores; El consejo dio como fecha límite de recepción de sugerencias hasta el 1 de octubre de 2007.

La diferencia más notoria de este último documento en comparación a las ya conocidas NIIF (denominadas en la Actualidad NIIF FULL, o para empresas Listadas) es que debido al volumen de transacciones , naturaleza de las operaciones y obligaciones de las PYMES, la normativa es menos compleja y establece parámetros generales que pueden adoptar para el registro de las transacciones; aunque al igual que sus antecesoras, dan lugar a la aplicación del criterio acorde a cada circunstancia que pueda enfrentar la entidad, ello en

función de revelar información financiera útil para la administración y demás usuarios de la misma.

1.2. PROCESAMIENTO ELECTRÓNICO DE DATOS

Desde épocas muy remotas el ser humano ha utilizado diferentes mecanismos para procesar los datos, el hombre primitivo empleaba los dedos de las manos para efectuar operaciones sencillas y almacenar toda la información posible en su memoria, siendo necesario auxiliarse de medios que le permitieran resolver operaciones complejas, uno de las primeras herramientas para el proceso de la información fue el ábaco, que consistía en una tabla con una serie de ranuras en donde son colocadas tantas fichas (indicadores) como unidades, decenas o centenas haya que representar. En la Europa Medieval se desarrollaron dispositivos llamados contadores, que se usaban con este objetivo.

En 1642 Blaise Pascal, inventó una máquina en la cual se utilizaba una rueda con diez dientes, que conectada a otra serie de ruedas podía sumar y restar. Siendo la base de la primera calculadora que llevaba el nombre de "Maquina Aritmética De Pascal O Pascalina"[2]

[2] La Evolución del Procesamiento de Datos, www.oni.escuelas.edu.ar, Buenos Aires, Argentina.

En 1671, Gottfried Wilhelm Von Leibiniz extendió el concepto para incluir operaciones de multiplicación, división, además de la opción de extraer raíces cuadradas.

En 1887, el Dr. Herman Hollerith desarrolló el registro de la información por medio de tarjetas perforadas. Previamente en 1812 Charles Babbage introdujo el principio de memoria, a través de una máquina que calculaba y retenía la información para ser usada en repetidas veces. [3]

En 1895, se utilizó la máquina de Herman Hollerith para la contabilidad de los ferrocarriles centrales de Nueva York y fue la primera aplicación comercial automática. Al ver los resultados se decidió la creación de la empresa Tabulating Machines Company en 1896 dando la Internacional Business Machines o IBM.

En 1937 el físico norteamericano John V. Atanasoff, junto a su colaborador Clifford Berry, construyeron una máquina electrónica que operaba en binario siguiendo la idea de Babbage. Fue la primera máquina de cálculo digital, puesto que no tomó carácter de computadora porque no existía la posibilidad de programarla.

[3] Procesamiento de Datos, www.pcm.gob.pe, Estados Unidos.

En el año de 1939 se desarrolló el computador Mark I, el cual utilizaba cintas perforadas que dirigían las máquinas para programar acciones. Más tarde en los años de 1944 John Von Neumann, desarrolló la idea de una computadora donde los programas no eran parte de ella, sino que se podían cambiar sin modificar el cableado llamado modelo Von Neumann, construyéndose por fin en 1952 una maquina basaba en este modelo llamado EDVAC (Electronic Discrete Variable Automatic Computer) (Computadora Automática Electrónica de Variable Discreta).

En 1951, fue construida por los creadores de ENIAC la primera computadora de serie, llamada UNIVAC-I y a partir de 1952 se fabricaron en serie como MANIAC-I, MANIAC-II y la UNIVAC-II.

En la actualidad el proceso electrónico de datos (PED) representa el principal avance técnico logrado en el mundo de los negocios. Los sistemas PED pueden manejar un gran número de diversas tareas, desde procesar una sencilla nomina hasta simular los efectos que diferentes alternativas de decisión producirían en todas las operaciones de una empresa.

El PED sé está aplicando audazmente a funciones de control de la función directiva, proporcionando una poderosa herramienta para aumentar la efectividad de sus procedimientos y prestar mayores

servicios a los clientes; dentro de los requisitos físicos necesarios para la aplicación de un adecuado PED, se encuentran los siguientes elementos:

Un sistema PED consta de los siguientes elementos:

a) Un procesador electrónico de datos (la unidad central de procesamiento).
b) Equipo periférico asociado, formado por dispositivos de preparación de datos, de entrada y salida, etc. Este elemento central ejecuta funciones lógicas, aritméticas y de almacenamiento de datos durante el proceso.
c) Procedimientos para indicar que datos se necesitan y cuando, así como donde obtenerlos y en qué forma utilizarlos.
d) Rutinas de instrucción para el procesador.
e) Personal para operar, conservar y mantener el equipo, estableciendo procedimientos, instrucciones, y verificando resultados en su totalidad.

1.2.1. Definiciones

a) Datos

Son las unidades elementales para la producción de la información. Los datos son la materia prima de los sistemas de procesamiento de datos que sirven de apoyo a los sistemas de

información. Funcionalmente, los datos son el registro de los hechos, cifras, palabras, símbolos, gráficas, etc. Que representan una idea, objeto, condición o situación. Consecuentemente, la información consiste en datos seleccionados y organizados con respecto al usuario, problema tiempo, lugar, y función.

b) El Procesamiento Electrónico de Datos (PED)

Se refiere al proceso electrónico de datos que forman parte de la organización de una empresa (divisiones, áreas o departamentos) y tiene por función verificar la exactitud e integridad del software, que procesa los datos así como la entrada y salida de datos generadas por las redes de los sistemas computacionales.

1.2.2. Tipos De procesamiento de datos

Para procesar la información contable se puede realizar según se describe a continuación:

a) Proceso manual.

Este es el proceso más antiguo que se conoce e involucra el uso de los recursos humanos, para realizar cálculos mentales, registrar, ordenar y clasificar los datos manualmente.

Esto da como resultado un proceso lento y expuesto a generar errores durante el ciclo de procesamiento. Finalmente los resultados se expresan de manera escrita, creando grandes volúmenes de información almacenada.

b) Proceso mecánico.

Se realiza por medio del uso de máquinas registradoras y calculadoras, reemplazando en cierto grado el tiempo aplicado durante el proceso de cálculo manual.

Esto simplifica el trabajo en relación al proceso y la reducción de errores, pero mantiene la desventaja del proceso de almacenamiento de toda la información resultante.

c) Proceso electromecánico.

En este tipo de proceso, el enlace de información entre los elementos de tratamiento, almacenamiento y comunicación, sigue realizándose de una forma manual, pero para realizar cada una de estas tareas se emplean máquinas electromecánicas, con las cuales se obtiene mayor eficiencia.

d) Procesos electrónicos.

En este tipo de proceso se emplean las computadoras y en un menor nivel la intervención humana que ingresa, clasifica y adecua la información.

Una vez que es ingresada, el computador efectúa los procesos requeridos automáticamente y permite el resultado deseado. Los procesos de calculo (matemáticos, aritméticos, lógicos, etc.), de ordenamiento, son realizados a velocidades increíblemente altas, obteniendo información confiable y precisa.

1.2.3. Clasificaciones del procesamiento electrónico de datos

a) Procesamiento por lotes.

Este se basa en la generación de archivos que constituyen batches de la base de datos principales, además necesita copia del software en la terminal que se utiliza, lo cual ocasiona costos por cada licencia.

Es conocido como batch o procesamiento por lotes, al modo de funcionamiento de un programa que se ejecuta en forma no interactiva sobre una gran cantidad de datos.

Generalmente se diseñan programas para su funcionamiento en "modo por lotes" cuando la misma tarea se debe aplicar a una gran cantidad de información.

b) Procesamiento en línea

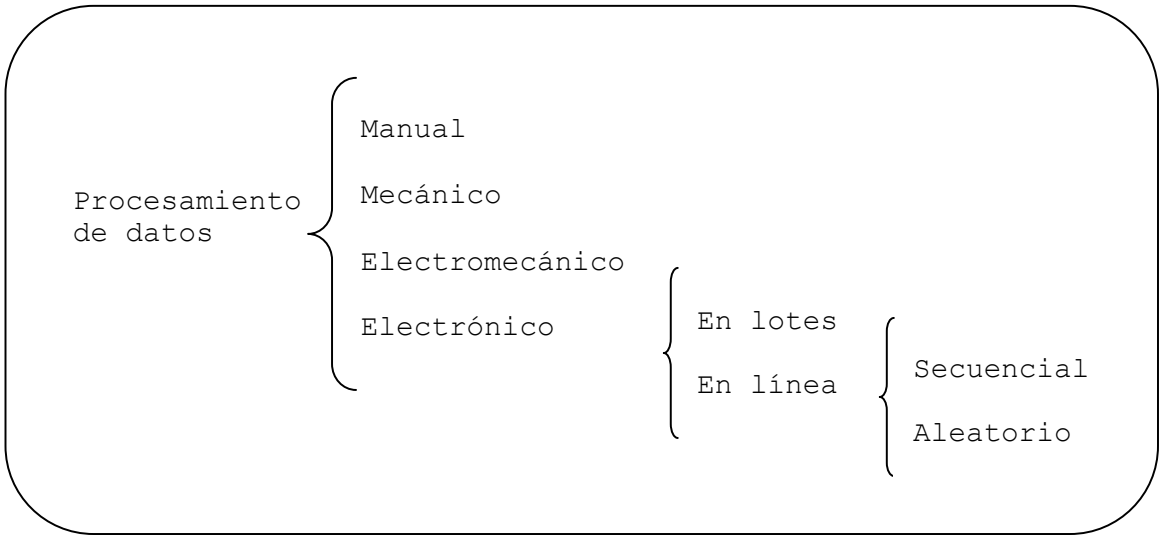
El procesamiento en línea implica que los programas se ejecuten de tal forma que los datos se actualicen de inmediato en los archivos de la computadora. A este tipo de procesamiento se le conoce también como tiempo real.

Sus aplicaciones son indispensables en aquellos casos en que los datos contenidos en los archivos se modifican varias veces en el transcurso de un día y se consultan en forma casi inmediata. Existen otros dos métodos reconocidos mediante los cuales los datos son procesados dentro de un sistema:

a) **Secuencial,** se aplica cuando los registros de archivos están en cadena tal como ocurre con las cintas magnéticas. En este tipo de procesamiento, el archivo debe ser leído por la computadora en cualquier ocasión en que una transacción se tenga que procesar.

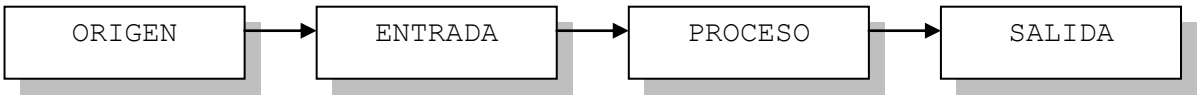
b) Aleatorio, las transacciones pueden ser procesadas en cualquier orden, pues en el archivo solo la cuenta específica se lee al procesar la transacción.

Grafico 2 : "Flujograma del Procesamiento Electrónico de Datos"



1.2.4. Ciclo básico del procesamiento electrónico de datos

El ciclo del PED consiste en un método sistemático para manejar datos y obtener la información deseada y consta de cuatro etapas:



a) Origen:

El origen de los datos es de vital importancia, esta etapa consiste en asegurar la veracidad, integridad, y confiabilidad de los datos que serán procesados.

Los controles que pueden ser aplicados en esta etapa son:

- **Procedimientos de preparación de datos:** Los departamentos implementan y dan seguimiento a los procedimientos de preparación de datos. En este contexto, el diseño de los formatos de entrada asegura que los errores y las omisiones se minimicen. Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable que los errores y las irregularidades son detectadas, reportadas y corregidas.
- **Procedimientos de autorización de documentos fuente:** El personal autorizado, actuando dentro de su autoridad, prepara los documentos fuente de forma adecuada y existe una segregación de funciones apropiada con respecto a la generación y aprobación de los documentos fuente.
- **Recolección de datos de documentos fuente:** Los procedimientos garantizan que todos los documentos fuente autorizados son completos y precisos, debidamente justificados y transmitidos de manera oportuna para su captura.

- **Manejo de errores en documentos fuente:** Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable la detección, el reporte y la corrección de errores e irregularidades.
- **Retención de documentos fuente:** Existen procedimientos para garantizar que los documentos fuente originales son retenidos o pueden ser reproducidos por la organización durante un lapso adecuado de tiempo para facilitar el acceso o reconstrucción de datos así como para satisfacer los requerimientos legales.

b) Entrada:

Consiste en la recopilación de todos los datos requeridos, ordenados para su procesamiento. Se pueden considerar como etapa importante en la función del registro de datos el proceso de edición, codificación, conversión y verificación.

Controles aplicables a la etapa de Entrada son:

- **Procedimientos de autorización de captura de datos:** Los procedimientos aseguran que solo el personal autorizado capture los datos de entrada.
- **Verificaciones de precisión, integridad y autorización:** Los datos de transacciones, ingresados para ser procesados (generados por personas, por sistemas o entradas de

interfases) están sujetos a una variedad de controles para verificar su precisión, integridad y validez. A la vez garantizan que los datos de entrada son validados y editados tan cerca del punto de origen como sea posible.

- **Manejo de errores en la entrada de datos:** Ante la existencia de errores se realizan procedimientos para la corrección y re-captura de datos que fueron ingresados de manera incorrecta.

c) Proceso:

Es la etapa en la cual se realizan o ejecutan todos los cálculos o pasos necesarios con los datos de entrada.

Dentro de la etapa del procesamiento se encuentran los siguientes controles:

- **Integridad en el procesamiento de datos:** Los procedimientos para el procesamiento de datos aseguran que la separación de funciones se mantiene y que el trabajo realizado de forma rutinaria se verifica. Los procedimientos garantizan que existen, controles de actualización adecuados, tales como totales de control de corrida-a-corrida, y controles de actualización de archivos maestros.
- **Validación y edición del procesamiento de datos:** Los procedimientos garantizan que la validación, la

autenticación y la edición del procesamiento de datos se realizan tan cerca como sea posible del punto de generación. Los individuos aprueban decisiones vitales que se basan en sistemas de inteligencia artificial.

- **Manejo de errores en el procesamiento de datos:** Los procedimientos de manejo de errores en el procesamiento de datos permiten que las transacciones erróneas sean identificadas sin ser procesadas y sin una indebida interrupción del procesamiento de otras transacciones válidas.

d) Salida:

Es el resultado del procesamiento de los datos o representación de la información deseada, los cuales son conocidos como informes obtenidos.

En la etapa de Salida, existen dos tipos de controles que pueden ser aplicados, lo que son los controles de salida y controles de límites:

- **Manejo y retención de salidas:** El manejo y la retención de salidas provenientes de aplicaciones de Tecnología de Información (TI), siguen procedimientos definidos y tienen en cuenta los requerimientos de privacidad y de seguridad.

- **Distribución de salidas:** Los procedimientos para la distribución de las salidas de TI se definen, se comunican y se les da seguimiento.
- **Cuadre y conciliación de salidas:** Las salidas cuadran rutinariamente con los totales de control relevantes. Las pistas de auditoría facilitan el rastreo del procesamiento de las transacciones y la conciliación de datos alterados.
- **Revisión de salidas y manejo de errores:** Los procedimientos garantizan que tanto el proveedor como los usuarios relevantes revisan la precisión de los reportes de salida. También existen procedimientos para la identificación y el manejo de errores contenidos en las salidas.
- **Provisión de seguridad para reportes de salida:** Existen procedimientos para garantizar que se mantiene la seguridad de los reportes de salida, tanto para aquellos que esperan ser distribuidos como para aquellos que ya están entregados a los usuarios.
- **Autenticidad e integridad:** Se verifica de forma apropiada la autenticidad e integridad de la información generada fuera de la organización, ya sea que haya sido recibida por teléfono, por correo de voz, como documento en papel, fax o correo electrónico, antes de que se tomen medidas potencialmente críticas.

- **Protección de información sensitiva durante su transmisión y transporte:** Se proporciona una protección adecuada contra accesos no autorizados, modificaciones y envíos incorrectos de información sensitiva durante la transmisión y el transporte

1.2.5. Ventajas y desventajas del procesamiento electrónico de datos

Para realizar un correcto registro de las operaciones y la toma de decisiones, la forma en que se procesen los datos puede afectar significativamente la estructura organizacional de una empresa, así como los procedimientos de control necesarios para satisfacer los amplios objetivos del control interno contable necesarios al procesar electrónicamente los datos, entre las ventajas y desventajas de este proceso se mencionan las siguientes:

a) Ventajas.

El procesar los datos de formar electrónica, presenta los siguientes beneficios:

- Maximiza el tiempo
- Se puede realizar un mejor trabajo con un gran número de distintas tareas.

- La reducción de los tiempos de procesamiento, para tener de forma oportuna y precisa la información requerida.
- Realiza una reducción en los costos que se aplican al momento de realizar el procesamiento de la información contable.
- Mejora la capacidad del recurso humano, para que estén en óptimas condiciones, para la utilización de los sistemas durante el procesamiento de la información.
- Cuenta con un nivel superior para realizar un mejor control para evitar la manipulación de la información.

b) Desventajas

- En el PED existe menos evidencia documental que en los sistemas manuales.
- El PED es más susceptible a fallas físicas, manipulaciones no autorizadas y funcionamiento mecánico deficiente en contraste con la información de los sistemas manuales.
- Con frecuencia los cambios en el sistema son más difíciles de implementar y de controlar en el PED con relación a los sistemas manuales.

1.2.6. Aspectos legales y técnicos relativos al procesamiento electrónico de datos

El procesamiento electrónico de datos (PED) , es parte del desarrollo de la tecnología informática, por medio de la cual brinda beneficios económicos, pero a su vez puede ocasionar un riesgo de daños a nivel material y moral, a través de la manipulación fraudulenta de las computadoras con ánimo de lucro, la destrucción de programas o datos, el acceso y la utilización indebida de la información, afectando la esfera de la privacidad y credibilidad de la información hacia terceras personas.

Para realizar el PED, se requiere de varios mecanismos e instrumentos necesarios, entre los cuales se debe considerar el uso de un adecuado sistema informático, para la ejecución del mismo, el cual debe cumplir con la normativa legal siguiente:

1.2.6.1. Aspectos legales

a) Código Civil

El Código, establece que al obtener un sistema informático se debe realizar, mediante la formalización de un contrato de servicios, en el cual se establezcan las cláusulas en que consten las obligaciones que adquieren los sujetos del mismo, por el plazo que se fija para su cumplimiento, éstas ultimas

dan derecho a exigirlo; y en tal sentido, el artículo 1351 las clasifica como obligaciones civiles.

Se puede determinar que para la obtención del sistema informático, se hace por medio de un contrato, el cual se determinan todos los aspectos que debe incluir el mismo para la realización adecuada del PED.

b) Código de Comercio

Considerando el sistema informático como un bien intangible[4], el código establece que se deberá incluir como parte del Activo de la sociedad.

Además en el Art. 435, expresa que: todo comerciante está obligado a llevar la contabilidad por medio de hojas separadas y efectuar las anotaciones en el diario en forma resumida y también podrán hacer uso de sistemas electrónicos o de cualquier otro medio técnico idóneo para registrar las operaciones contables.

c) Ley de Fomento y Protección de la Propiedad Intelectual

En el contrato de PED se puede establecer, que el prestador de servicios sea quien proporcione el sistema de información, por

[4] Bien Intangible el cual puede ser una Patente ò Marca

lo tanto en la celebración de este tipo de contratos, la parte contratante debe asegurarse que la contratada que proporciona el sistema posee los derechos patrimoniales para la explotación del mismo.

También nos menciona el tiempo en que deberá legalizarse el sistema informático y en el Art. 89 nos explica las penalidades que deberá de realizarse por la violación a los derechos de autor por utilizar de forma indebida el sistema informático.

d) Ley de Impuesto Sobre la Renta

En esta Ley y su Reglamento de Aplicación no se define expresamente el concepto de contrato de PED, sin embargo por tratarse de la prestación de un servicio generador de rentas gravables es comprendido dentro del artículo 1 de la misma, el que establece que la obtención de rentas por los sujetos pasivos en el ejercicio o período de imposición, en el que se trate genera la obligación de pago del correspondiente impuesto.

Además se debe considerar que el sistema informático es un bien intangible y por lo tanto en el Art. 30 A, nos determina

el porcentaje legal para su respectiva amortización, a que debe ser objeto el sistema informático.

1.2.6.2. Aspectos técnicos

a) COBIT 4.0

Es una normativa técnica que ha sido desarrollada para componer un marco de trabajo de dominios y procesos, la cual nació por la necesidad de contar con un sistema de información que tuviera un marco de control y de gestión de los SITIC (Sistemas de Información y Tecnologías de la Información y las Comunicaciones), que garantizara que se cumpliesen los objetivos de la organización reduciendo los riesgos y generando valor para la entidad.

COBIT se divide en tres niveles:

1. Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
2. Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control.
3. Actividades: Acciones requeridas para lograr un resultado medible.

En el procesamiento electrónico de datos (PED), debe aplicarse la división de Dominios, la cual se compone de la siguiente manera:

1. Dominio: Planificación y organización.
2. Dominio: Adquisición e implementación.
3. Dominio: Prestación y soporte,
4. Dominio: Monitoreo

COBIT brinda para el PED en su marco de referencia denominado, **Procesos de la entrega y soporte (DS)**, algunos objetivos de control orientados a garantizar la seguridad de los sistemas y los datos manipulados en los mismos, entre los cuales se pueden mencionar los siguientes:

DS5.1 Administración de la seguridad de TI
DS5.2 Plan de seguridad de TI
DS5.3 Administración de identidad
DS5.4 Administración de cuentas del usuario
DS5.5 Pruebas, vigilancia y monitoreo de la seguridad
DS5.7 Protección de la tecnología de seguridad
DS5.8 Administración de llaves criptográficas
DS5.11 Intercambio de datos sensitivos

También son aplicables los requerimientos de seguridad para la administración de datos enmarcados en el DS11.6.

1.3. Seguridad informática

En la Actualidad la seguridad informática en el mundo, ha tomado gran auge debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles, la posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad, y poder explorar más allá de las fronteras nacionales, lo cual ha llevado a la aparición de nuevas amenazas para los sistemas de información, es decir que los grandes beneficios proporcionados por la tecnología, solo puede ser equiparable con el alto precio que muchas empresas han sufrido en las últimas décadas, por un inadecuado uso de los sistemas de información y la tecnología. Ello aunado a los mencionados casos de fraude o delitos informáticos en grandes empresas, y a las pérdidas millonarias en información, que miles de ellas han sufrido producto de una intromisión de un virus informático. Estos riesgos que enfrentan las mismas las han llevado a desarrollar documentos y directrices orientadas al uso adecuado de las destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas, evitando el uso indebido.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y

sensibilidad de la información que permite a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar en función del dinámico ambiente que rodea las organizaciones modernas.

Es por ello que en la década de los 80`s la organización y desarrollo económico, inicio esfuerzos con la finalidad de unificar esfuerzos a nivel internacional para disminuir el uso y abuso que se hace de programas informáticos por medio de mejores regulaciones legales siendo de esta manera que la **OCDE** (Organización para la Cooperación y el Desarrollo Económico) categoriza como delito informático, cualquier comportamiento antijurídico no ético, y no autorizado relacionado con el procesamiento informático de datos y/o su transmisión.

Adicionalmente esta organización brindo un conjunto de normas para la seguridad informática con la finalidad de proporcionar para muchos países las bases de un marco de seguridad para los sistemas informáticos.

La ONU define los delitos informáticos en 3 categorías

a) Fraudes cometidos mediante la manipulación de computadoras
b) Manipulación de los datos de entrada
c) Daños o modificaciones de trabajos computarizados

En la actualidad, han surgido muchos movimientos, para frenar y normar aquellos delitos que se dan en la red a nivel mundial, entre estos esfuerzos se pueden mencionar:

En Venezuela, en forma conjunta las empresas Venamcham y Cavecom, vinculadas al desarrollo de las telecomunicaciones, decidieron elaborar una ley donde se garantice la seguridad jurídica, sobre los mensajes de datos transmitidos electrónicamente, la cual se denomino "Ley de Mensaje de Datos y Firmas Electrónicas", y fue aprobada por el Consejo de Ministros el 10 de febrero de 2000.

En España se han adoptado diversas normativas que contribuyen al respaldo de la información digitalizada, entre las cuales se pueden mencionar:

a) Real Decreto-Ley 14/1999,
b) Firma Electrónica y Directiva 1999/93
c) Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico.

La Organización Internacional de Estandarización (ISO), en el año 2005, lanzó su conjunto de Normas 27000, que establecen una implementación efectiva de la seguridad de la información empresarial.

En México, el 29 de Mayo de 2000 se publican en el Diario Oficial Federal el decreto en que se reforman y adicionan diversas disposiciones del Código Civil, Código de Comercio y Ley Federal de Protección al Consumidor, donde se realizan modificaciones y adiciones para regular los actos celebrados en materia civil y mercantil utilizando medios electrónicos.

En El Salvador se han dado muchos impulsos para incrementar la seguridad informática, entre los cuales pueden mencionar la creación de la "Ley de Fomento y Protección de la Propiedad Intelectual" (Decreto Legislativo No. 604 del 15 de julio de 1993) y su respectivo reglamento (Decreto Legislativo No. 35 del 18 de septiembre de 1994), en el cual se incluyes y protege a los programas de ordenador, de muchos delitos informáticos como la piratería; otros de los esfuerzos más notorios son las últimas reformas al Código Procesal Penal (Decreto Legislativo No.386 del 16 de Agosto de 2007) en el cual se regulan y tipifica varios delitos informáticos; El más reciente esfuerzo es la creación de "La Comisión Nacional para la Sociedad de la

Información de El Salvador", la cual tiene como objetivo motivar la implementación de las TIC como medio de desarrollo en las empresas y regular en uso de transferencias electrónicas de información; esta comisión se prevé que comience sus funciones en el año 2009.

1.3.1. Factores que afectan la seguridad informática

La pérdida de la seguridad informática es ocasionada por diversos factores, algunos de los cuales pueden ser controlados por el hombre, y otros no, un ejemplo de los primeros es cuando la dirección empresarial se encuentra a cargo de la debida protección de las instalaciones del centro de cómputo. A la vez existen otras causas que no pueden ser controladas por ellos, como lo son los desastres naturales, incendios robos, etc. Por tal motivo, se apreciaran las dos grandes categorías que intervienen en la seguridad informática a continuación:

1.3.1.1. Factores Externos

Son aquellos factores que intervienen por ingerencias externas a la empresa, los cuales no son controlables, entre los que se mencionan los atribuibles a casos fortuitos o de fuerza mayor, y errores humanos de tipo voluntario o involuntario.

La mayoría de estos no tienen medidas para evitar sus intromisiones al interior de la entidad, por lo que se deben adoptar medidas de contingencias para hacer frente a los posibles efectos derivados de estos fenómenos.

La clasificación que el "Establecimiento del Sistema Nacional de Protección Civil" mexicano, realiza ante los casos fortuitos o de fuerza mayor son:

a) Geológicos: Tiene sus orígenes en las placas tectónicas y fallas continentales. Entre los desastres más comunes se pueden mencionar:
   - Sismos
   - Vulcanismo
   - Colapso del suelo
   - Hundimiento regional y agrietamiento, etc.

b) Hidrometeorológicas: Se da por los distintas clases de acciones violentas derivadas de agentes atmosféricos, entre los cuales se mencionan:
   - Lluvias
   - Huracanes
   - Tormentas con granizo
   - Inundaciones

- Temperaturas extremas
- Sequías
- Tormentas eléctricas
- Vientos, etc.

c) Químicos: Se encuentran ligadas directamente al desarrollo industrial y tecnológico y al uso de diversas formas de energía, por lo general afecta en mayor medida a las grandes concentraciones humanas e industriales. Las cuales son:

- Contaminaciones
- Envenenamientos
- Incendios
- Explosiones
- Radiaciones, etc.

d) Socio – organizativos: Tiene su origen en las actividades de las concentraciones humanas y en el mal funcionamiento de algunos sistemas de subsistencia que proporciona servicios básicos, entre los que se mencionan:

- Fallas humanas
- Disturbios sociales
- Actos delictivos

- Accidentes
- Acciones bélicas
- Interrupción de servicios, etc.

1.3.1.2. Factores Internos

Son aquellos en que intervienen los sistemas de información y los componentes tecnológicos que soportan las operaciones de la mayoría de empresas y organizaciones.

Aunque estos factores pueden ser mayormente controlados por las empresas, también pueden producir efectos devastadores; por lo cual, deben de identificarse los riegos potenciales.

Entre las principales áreas, que las empresas deben abordar, para identificar aquellas situaciones que ponen en riesgo la seguridad de la información están:

a) Las instalaciones físicas: es el lugar donde se encuentra situada la máquina o centro de cómputo, normalmente es conocido como "el entorno de la computadora".
b) Los procesamientos operacionales: son aquellos utilizados para hacer uso del computador.
c) El hardware: Se refiere al equipo de cómputo en sí.
d) Las redes y comunicaciones: son aquellos periféricos a los que las computadoras están conectados, para realizar la

transferencia de información, ya sea dentro o fuera de la empresa.

e) El software: Es la parte lógica o intangible de las computadoras, y son todos aquellos programas y sistemas operativos que hacen funcionar al hardware.

1.3.2. Áreas en que se divide la seguridad informática

La seguridad informática no solo se limita a las medidas que se deben ejecutar al usar programas computarizados, sino que debe orientarse a salvaguardarla de los diversos factores que ponen en riesgo la información, entre los cuales se pueden mencionar el mal estado del equipo de cómputo, los virus, el espionaje por Internet, etc. Para poder dar una mejor cobertura a estos riesgos se clasifica en tres grandes áreas que son:

1.3.2.1. Seguridad Física

La seguridad física se define como "un conjunto de lineamientos y procedimientos cuyo objetivo es evitar o disminuir la exposición a riesgos, ya sean internos o externos en las instalaciones físicas del centro de cómputo."[5]

Estos lineamientos y procedimientos deben estar encaminados a proteger las instalaciones, comunicaciones, equipos de cómputo y

[5] Seguridad de la Información en Sistemas de Cómputo, Luís Ángel Rodríguez Año 1995, Ventura Ediciones, S.A. DE C.V.

redes (Hardware), tomando en cuenta riesgos como: desastres naturales, ataques de intrusos, condiciones ambientales, etc.

Entre los fenómenos que se dan, y que afectan de forma directa a la seguridad física están:

- Desastres Naturales y de Origen Mixto (naturales o provocadas por el hombre), ejemplo de estos son los incendios e inundaciones.
- Riesgos de Control Ambiental, ejemplo de estos son la falla de corriente eléctrica, fallas en el sistema de aire acondicionado y la contaminación.
- Acciones Deliberadas, ejemplos de este se pueden mencionar el robo de equipo e información, actos destructivos premeditados y amenaza de los vecinos.

Los controles utilizados para salvaguardar la seguridad física, se delimita en tres diferentes enfoques:

a) Preventivos: son aquellas actividades y políticas encaminadas a advertir que un riesgo se vuelva en una calamidad.
b) Detectivos: son aquellas actividades y políticas encaminadas a revelar que actos, originaron una calamidad o error, estos son aplicados posteriormente de ocurrido dicho suceso.

c) Correctivos: estos sirven para enmendar los efectos negativos derivados de fenómenos ocurridos, en algunos casos son imposibles implementarlos.

1.3.2.2. Seguridad Lógica

La seguridad lógica se define como "el establecimiento de políticas generales y controles que previenen o detectan cualquier intento de acceso no autorizado a un sistema de cómputo."[6]

Este tipo de seguridad es tan importante como la física, ya que incluye las normas para el control de acceso de datos y/o información, a fin de minimizar el riesgo de transferencia, modificación, pérdida o divulgación accidental o intencional de estos.

Entre los fenómenos que afectan de forma directa a la seguridad lógica se pueden mencionar:

- Riesgos debido a la amigabilidad de los sistemas
- Riesgos debidos a la conectividad de los sistemas
- Riesgo a la prevacía
- Riesgo en la integridad de la información

---

[6] Seguridad de la Información en Sistemas de Cómputo, Luís Ángel Rodríguez Año 1995, Ventura Ediciones, S.A. DE C.V.

- Riesgo en la confiabilidad del personal
- Riesgo de errores en el software
- Riesgo de errores en los datos
- Desempeño inadecuado del sistema
- Piratería de software
- Crimen por computadora

Los tipos de controles que se pueden implementar en la seguridad lógica se pueden hacer con los mismos enfoques que toma la seguridad física.

1.3.2.3. Seguridad en redes y comunicaciones

La definición de Seguridad en redes y comunicaciones implica tres aspectos básicos de protección:

a) Proveer acceso controlado a los recursos (identificar y autentificar).
b) Proveer el uso controlado de esos recursos; y
c) Proveer la seguridad de que el nivel de protección deseado es alcanzado.7

[7] Seguridad de la Información en Sistemas de Cómputo, Luís Ángel Rodríguez Año 1995, Ventura Ediciones, S.A. DE C.V.

Entre los fenómenos que afectan de forma directa a la seguridad en redes y comunicaciones se pueden mencionar:

- Intercepción: la cual puede ser pasiva (la que captura datos sin modificarse, por ejemplo el espionaje y el análisis de tráfico), activa (en la que el atacante realiza acciones para interferir los datos que se están transmitiendo, como modificación, borrado, inyección de mensajes falsos, retardo, etc.) y ataques accidentales (como pérdida de mensaje, duplicidad del mensaje, corrupción de mensaje, entre otros).
- Daños a infraestructura externa: Es un daño a la compañía que presta el servicio de comunicaciones.

Los controles que se pueden implementar para erradicar los riesgos de la seguridad en redes y comunicaciones, son los mismos que en las dos áreas anteriores.

1.3.3.Normativa legal

1.3.3.1. Normativa legal

En El Salvador aun no existe una ley especializada que regule los actos y delitos, realizados por medio de una computadora de forma directa, pero entre las leyes que tratan de mantener controlados los delitos informáticos más comunes, se pueden mencionar:

a) Ley de Fomento y Protección de la Propiedad Intelectual

La presente normativa hace un mayor énfasis a la protección de delitos informáticos en dos grandes puntos, los cuales son la protección a la propiedad intelectual (la cual está enmarcada principalmente en salvaguardar los derechos del autor) y a la sustracción de información clasificada (como lo son los secretos industriales y comerciales).

Los artículos con mayor énfasis en la propiedad intelectual se mencionan:

- Art. 33 Establece que el contrato entre los autores del programa de ordenador y el productor implica que le concede los derechos y exclusividad de los derechos patrimoniales, así como la autorización para su divulgación al productor de este, a menos que se establezca lo contrario en el contrato.
- Artículo 56. Enmarca que tanto los contratos de cesión y licencia de uso, deben hacerse por escritura publica, inscribirse en el Registro de Comercio y los contratos otorgados en el extranjero para que surjan efectos en El Salvador deben autenticarse y en su caso traducirse al castellano. Siempre respetando las formalidades establecidas acorde al lugar de su celebración.

- Articulo 58. Proporciona una lista de los requisitos que deben contener los contratos; tales como:
  a) Identificación del autor, el editor y la obra
  b) Si es inédita o no
  c) El numero de ediciones autorizadas
  d) Plazo para circulación de ejemplares de única o primera edición
  e) Cantidad de ejemplares en la edición, entre otros.

b) Código Procesal Penal

Esta ley enmarcada en el contexto de la seguridad informática, menciona en el Art. 184-A; que al tratarse de delitos contra derechos de propiedad intelectual, el juez o tribunal, aplicarán las siguientes medidas:

- ”La incautación de las mercancías presuntamente falsificadas o pirateadas, todos los materiales y accesorios utilizados para la comisión el delito, todo activo relacionado con la actividad infractora y toda evidencia documental relevante al delito. Los materiales sujetos a incautación en dicha orden judicial no requerirán ser identificados individualmente siempre y

cuando entren en las categorías generales especificadas en la orden;

- El decomiso de todo activo relacionado con la actividad infractora;
- El decomiso y destrucción de toda mercancía falsificada o que infrinja el derecho de autor o derechos conexos, sin compensación alguna al demandado, con el fin de evitar su ingreso en los canales comerciales; y
- El decomiso y destrucción de los materiales e implementos utilizados en la creación de la mercancía infractora."[8]

Además cabe mencionar que dicho código establece que estos delitos pueden ser penados de 6 meses hasta 8 años de prisión.

1.3.3.2. Normativa Técnica

Entre las normativas técnicas que tratan los procedimientos idóneos para mantener un ambiente de seguridad y entorno a la informática se pueden mencionar:

[8] Código Procesal Penal de El Salvador, Decreto Legislativo No. 450, de fecha 11 de octubre de 1973, publicado en el Diario Oficial No. 208, Tomo 241 del 9 de noviembre de 1973.

a) COBIT 4.0

Es una normativa que ha sido desarrollada por consensos obtenidos de expertos en la materia de las Tecnologías de la Información(TI), la cual se compone en un marco de trabajo de dominios y procesos, mayormente enfocados al control y no a los procesos.

Se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI. Estos procesos están agrupados en cuatro grandes dominios que se detallan a continuación junto con sus procesos y una descripción general de las actividades de cada uno:

5. Dominio: Planificación y organización, compuesto por los siguiente procesos:
   - PO1 Definición de un plan estratégico
   - PO2 Definición de la arquitectura de información
   - PO3 Determinación de la dirección tecnológica
   - PO4 Definición de la organización y de las relaciones de TI
   - PO5 Manejo de la inversión
   - PO6 Comunicación de la dirección y aspiraciones de la gerencia
   - PO7 Administración de recursos humanos

- PO8 Asegurar el cumplimiento con los requerimientos externos
- PO9 Evaluación de riesgos
- PO10 Administración de proyectos
- PO11 Administración de calidad.

6. Dominio: Adquisición e implementación, el cual tiene los siguientes procesos:
   - AI1 Identificación de soluciones automatizadas
   - AI2 Adquisición y mantenimiento del software aplicativo
   - AI3 Adquisición y mantenimiento de la infraestructura tecnológica
   - AI4 Desarrollo y mantenimiento de procedimientos
   - AI5 Instalación y aceptación de los sistemas
   - AI6 Administración de los cambios.

7. Dominio: Prestación y soporte, el cual esta compuesto por los siguientes proceso:
   - Ds1 Definición de niveles de servicio
   - Ds2 Administración de servicios prestados por terceros
   - Ds3 Administración de desempeño y capacidad
   - Ds4 Asegurar el servicio continuo
   - Ds5 Garantizar la seguridad de sistemas

- Ds6 Educación y entrenamiento de usuarios
- Ds7 Identificación y asignación de costos
- Ds8 Apoyo y asistencia a los clientes de TI
- Ds9 Administración de la configuración
- Ds10 Administración de problemas
- Ds11 Administración de datos.
- Ds12 Administración de las instalaciones
- Ds13 Administración de la operación.

8. Dominio: Monitoreo, el cual tiene los siguientes procesos:

- M1 Monitoreo del proceso
- M2 Evaluar lo adecuado del control interno
- M3 Obtención de aseguramiento independiente
- M4 Proveer auditoria independiente[9]

b) ISO 27000

La Organización Internacional de Estandarización (por sus siglas en inglés ISO), es una entidad encargada de emitir normas para obtener certificación de calidad en los controles de las empresas.

[9] COBIT 4.0

Esta organización ha realizado un gran número de normativas, entres las primeras que se pueden mencionar, en materia de seguridad informática está la norma BS7799, la que aparece por primera vez en 1995, con objeto de preparar a cualquier empresa –británica o no, en la certificación de la gestión de la seguridad de su información, por medio de una auditoria realizada por un auditor acreditado y externo; esta normativa constaba de dos partes, una es la guía de buenas prácticas y la otra parte que audita y certifica las empresas.

Posteriormente se hace una revisión de esta normativa, en el año de 1999 y nace la primera ISO 17799, las cuales son utilizadas por un gran número de empresa y acoge a las que ya se habían certificado con la norma BS7799.

Luego la norma ISO 17799 es revisada nuevamente, en el año 2005 y surge la nueva serie de ISO 27000.

Esta serie esta compuesta por las siguientes normativas:

- **ISO/IEC 27000:** Fundamentos y vocabulario. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

- **ISO/IEC 27001:** Norma que especifica los requisitos para la implantación del sistema de gestión de seguridad de la información (SGSI). Es la norma principal de requerimientos del sistema de gestión de seguridad de la información.
- **ISO/IEC 27002 (actualmente ISO/IEC 17799-2005):** Código de buenas prácticas para la gestión de seguridad de la información.
- **ISO/IEC 27003:** Directrices para la implementación de un sistema de gestión de seguridad de la información. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA (acrónimo inglés de Plan-Do-Check-Act: Planificar-Hacer-Verificar-Actuar) y de los requerimientos de sus diferentes fases.
- **ISO/IEC 27004:** Métricas para la gestión de seguridad de la información. Especificará las métricas y técnicas de medida aplicables para determinar la eficiencia y efectividad de la implantación de un SGSI y de los controles relacionados.
- **ISO/IEC 27005:** Gestión de riesgos de la seguridad de la información. Consistirá en una guía para la gestión del

riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI.

- **ISO/IEC 27006:** Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Especificará el proceso de acreditación de entidades de certificación y el registro de SGSI’s.

CAPITULO II

METODOLOGIA DE LA INVESTIGACION

2.1. Diseño metodológico

La investigación se desarrolló utilizando el método hipotético deductivo cuantitativo, el cual concibe la posibilidad de estudiar un fenómeno a partir de los datos numéricos, dichos datos son recolectados a través de cuestionarios y entrevistas, para la tabulación y análisis de ellos.

Bajo este enfoque, el desarrollo del trabajo de graduación estuvo orientado a explicar el porqué del comportamiento del fenómeno a investigar; de los problemas que tienen las medianas empresas del sector comercio de San Salvador en el procesamiento electrónico de datos contables, ocasionada por la carencia de políticas de seguridad informática.

2.1.1.Tipo de estudio

La investigación se basó en un estudio de tipo correlacional, el cual persigue, medir el grado de relación existente entre el riesgo de manipulación de la información contable y la ausencia de políticas de seguridad informática en el procesamiento electrónico de datos, con la finalidad de determinar la

influencia que una ejerce sobre la otra, y las vinculaciones existentes entre las variables expuestas.

En tal sentido, se llevó a cabo este tipo de estudio en las medianas empresas del sector comercio ubicadas en la zona de San Salvador, con la finalidad de evaluar la implementación y utilización de políticas de seguridad informática en el procesamiento electrónico de datos contables; así como el conocimiento y la adecuada preparación que posee el contador público, sobre esta problemática.

2.1.2.Recolección de la información

a) Documental

Esta consistió en la revisión y análisis de la literatura fuente, que comprende las leyes y reglamentos relacionados, normas de Calidad (ISO 27000 e ISO 17799), libros, trabajos de graduación, boletines y revistas, etc.

b) Virtual

Información obtenida de páginas web y el ciberespacio.

c) De campo

Se utilizó el cuestionario como instrumento de recolección de datos, dirigido a los contadores de las empresas objetos de

estudio, para medir el conocimiento que poseen con respecto a la implementación de manuales de seguridad informática; también se utilizó las entrevistas al personal involucrados en el procesamiento electrónico de datos, para determinar las actividades que efectúan en el procesamiento de la información contable, y determinar las deficiencias que hay en dichos procedimientos.

2.1.3. Unidades de análisis

a) Universo

La población para esta investigación se encuentra conformada por un total de 82 empresas del municipio de San Salvador, la información se obtuvo, por medio de las medianas empresas del sector comercio, que utilizan recursos tecnológicos para el procesamiento electrónico de datos contables en Sistemas Computarizados, y a las personas que ejecutan dicha función al interior de las entidades mencionadas.

b) Muestra

De acuerdo al universo se empleó un prototipo probabilística, tomando en cuenta que la población es finita Para la selección de la muestra se utilizó el método aleatorio simple, que consiste en que todos los elementos de la población tienen la misma probabilidad de ser escogidos.

Los elementos que se tomaron como referencia son los registros recabados por la Cámara de Comercio e Industria de El Salvador, de las empresas del sector comercio del municipio de San Salvador al 30 de abril del año 2006; y el directorio de establecimientos proporcionado por la Dirección General de Estadísticas y Censos correspondiente al año 2005.

CAMARA DE COMERCIO E INDUSTRIA DE EL SALVADOR

TOTAL ASOCIADOS DISTRIBUIDOS POR FILIAL AL 30 DE ABRIL DE 2006

FILIAL	NUMERO DE EMPRESAS	% TOTAL DE SOCIOS
SAN SALVADOR	1128	61.2
SANTA ANA	266	14.4
SAN MIGUEL	299	16.2
SONSONATE	149	8.1
TOTAL	1842	100.00%

NUMERO DE EMPRESAS POR SECTOR Y TAMAÑO AL 30 DE ABRIL DE 2006

	TAMAÑO DE LA EMPRESA			
SECTOR	GRANDE	MEDIANA	PEQUEÑA	TOTAL GENERAL
AGROINDUSTRIA	6	12	37	55
COMERCIO	31	134	776	941
CONSTRUCCION	2	5	21	28
FINANCIERO	7	22	34	63
INDUSTRIA	7	40	129	176
SERVICIOS	13	40	450	503
TRASPORTE	0	6	23	29
TURISMO	3	4	40	47
TOTAL GENERAL	69	263	1510	1842

Para establecer el número de medianas empresas del sector comercio del departamento de San Salvador se toman los siguientes datos

Cuadro 1

FILIAL	**NUMERO DE EMPRESAS**	**% TOTAL DE SOCIOS**
SAN SALVADOR	1128	61.2%

Cuadro 2

	TAMAÑO DE LA EMPRESA			
SECTOR	**GRANDE**	**MEDIANA**	**PEQUEÑA**	**TOTAL GENERAL**
COMERCIO	31	134	776	941

Luego (134)(61.2%) = 82 empresas

La fórmula ha utilizar será la siguiente[10]:

$$n = \frac{Z^2 Npq}{(N-1)e^2+Z^2pq}$$

[10] Muestra finita. Bonilla, Gilberto. "Como hacer una tesis con técnicas estadísticas". UCA Editores.

n	=	Muestra	¿?
N	=	Universo	82
Z	=	Nivel de Confianza	1.96
P	=	Probabilidad de éxito 1	0.95
Q	=	Probabilidad de fracaso (1- P)	(1 – 0.95)
e	=	Margen de error	0.05

Al sustituir los datos en la fórmula se obtuvo el tamaño de la muestra:

$$n = \frac{(1.96)^2\,(82)(0.95)(1-0.95)}{(82-1)(0.05)^2 + (1.96)^2\,(0.95)(1-0.95)}$$

$$n = \frac{14.963032}{0.384976}$$

$$n = 34.3996 \text{ aprox. } 35 \text{ empresas}$$

2.1.4. Métodos e instrumentos de recolección de datos

a) Cuestionario

Los datos se obtuvieron por medio de un cuestionario que contiene preguntas abiertas y cerradas, el cual se pasó a los

Contadores y auxiliares contables de las empresas, involucradas en la presenten investigación.

b) Entrevistas

Las entrevistas se realizaron de forma aleatoria (máximo 5 empresas), a las personas que se encuentran directamente relacionadas con el procesamiento electrónico de datos contables al interior de las entidades involucradas en la investigación.

c) Observaciones

Se utilizó la técnica de la observación en la ejecución de la investigación y al implementar los instrumentos en las entidades, para apreciar y considerar aquellos aspectos y datos que puedan brindar más elementos e información al presente trabajo de investigación.

d) Análisis e interpretación

Se procedió a analizar e interpretar la información obtenida de cada pregunta formulada; esto sirvió para llegar a un diagnóstico del estado que se encuentran los sujetos de estudio.

2.2. Análisis de datos y diagnóstico

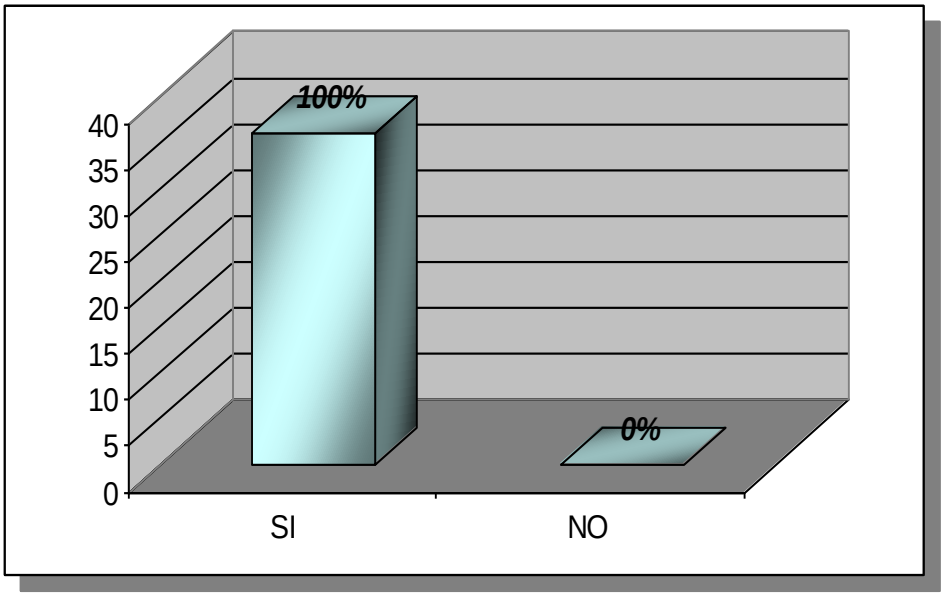
2.2.1. Análisis de datos

PREGUNTA No.1
¿Procesa Información contable en computadoras?

OBJETIVO: Identificar si el usuario se encuentra familiarizado con el procesamiento electrónico de datos contables en la computadora o si lo realizan de forma manual.

TABLA No. 1
UTILIZACION DE COMPUTADORAS PARA PROCERSAR INFORMACION CONTABLE

REPUESTAS	*FRECUENCIA*	*%*
SI	36	100.00%
NO	0	0.00%
TOTAL	**36**	**100.00%**



ANALISIS
Como se observa en la tabulación, hoy en día, el uso de una computadora es imprensindible para la manejo de la información; por tal motivo en un 100% de los usuarios encuestados afirman que el procesamiento de los datos contables lo realizan de forma computarizada.

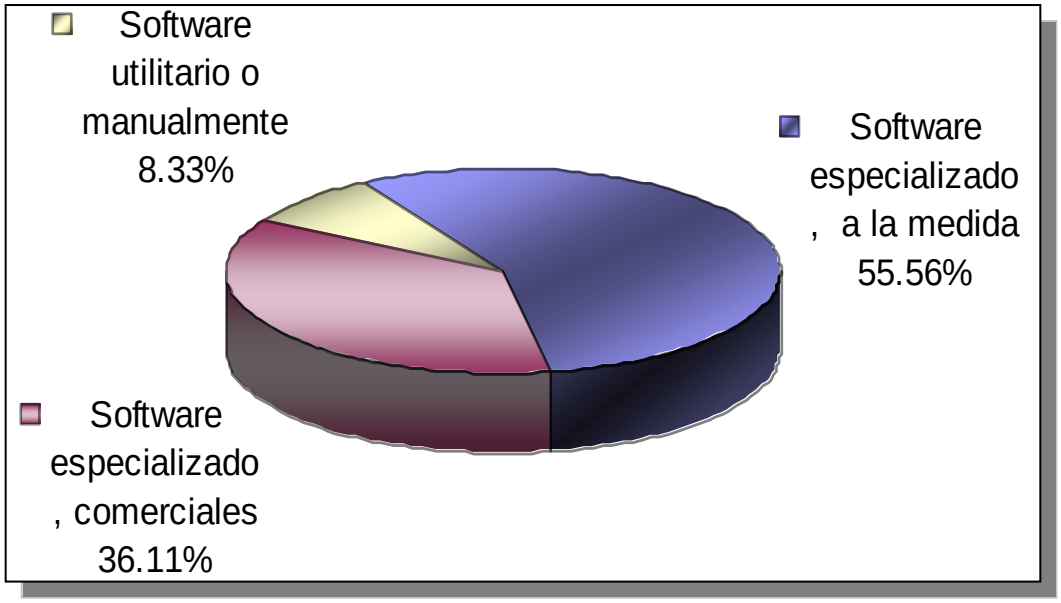
PREGUNTA No.2
¿En que tipo de programas procesa la información contable?

OBJETIVO: Determinar si el usuario hace uso de programas especializados para procesar la información contable, o hace uso de los programas comerciales que ofrecen las diferentes plataformas

TABLA No.2

SISTEMAS UTILIZADOS PARA PROCESAR LA INFORMACION CONTABLE

REPUESTAS	*FRECUENCIA*	*%*
Software especializado, a la medida	20	55.56%
Software especializado, comerciales	13	36.11%
Software utilitario o manualmente	3	8.33%
TOTAL	**36**	**100.00%**



ANALISIS

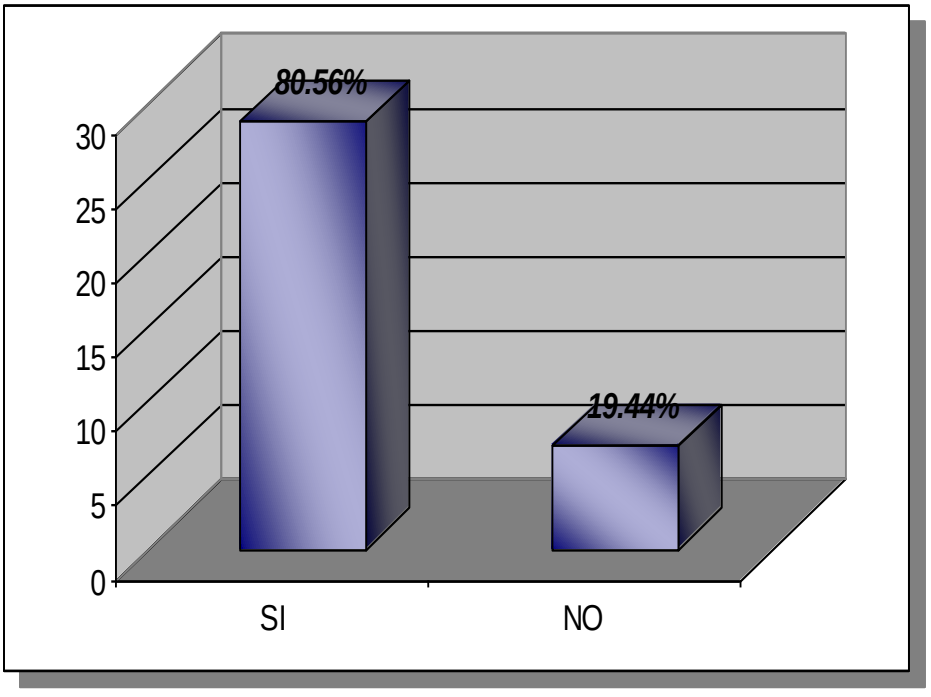
El 55.56% de los usuarios expresó que el software que utilizan son los especializados, es decir hechos a la medida, brindándoles mayores beneficios al momento de realizar sus operaciones contables y el 36.11% de los usuarios expresó que el software que la empresa utiliza es especializado de tipo comercial.

PREGUNTA No.3
¿Conoce en que consiste el término Seguridad Informática?

OBJETIVO: Identificar el nivel de conocimiento que el usuario posee acerca de seguridad informática.

TABLA No.3
CONOCIMIENTO SOBRE "SEGURIDAD INFORMATICA"

REPUESTAS	*FRECUENCIA*	*%*
SI	29	80.56%
NO	7	19.44%
TOTAL	**36**	**100.00%**



ANALISIS

Se observa que los usuarios que poseen una noción de lo que significa seguridad informática representa un 80.56%, esto se puede justificar por que, la informática se ha convertido en una herramienta indispensable en el que hacer empresarial.

PREGUNTA No.4

¿Qué tipos de procesos o políticas implementa para resguardar la información procesada electrónicamente?, mencione las 5 que considere más importantes.

OBJETIVO: Conocer si se aplican Políticas orientadas a la Seguridad Informática que el Usuario implemente en el PED, y verificar que las mismas sean acordes al objeto en estudio.

TABLA No 4
POLITICAS IMPLEMENTADAS PARA RESGUARDAR INFORMACIÓN

REPUESTAS	*FRECUENCIA*	*%*
Back up	26	32.05%
Claves de acceso	20	28.21%
Adquisición y mantenimiento de antivirus	15	17.95%
Adecuada segregación de Funciones	11	16.66%
Uso de servidores	6	5.13%
TOTAL	**78**	**100.00%**

ANALISIS

Entre las políticas que se utilizan para resguardar la información contable los usuarios consideran las siguientes: generación de back up, creación de claves de acceso, adquisición y actualización de antivirus, Uso de Servidores y la delimitación del personal autorizado a la información.

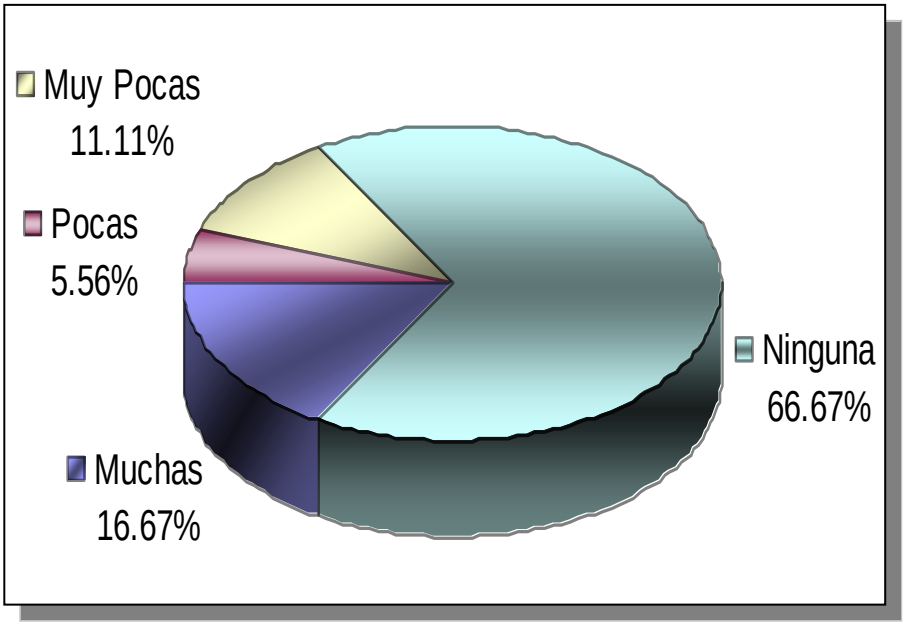
PREGUNTA No.5

¿Cuántas de esta y otras políticas o procedimientos están plasmadas en un Manual?

OBJETIVO: Determinar si el usuario cuenta con un Manual orientado a la Seguridad Informática.

TABLA No.5
EXISTENCIA Y APLICACIÓN DE POLITICAS DE SEGURIDAD INFORMATICA EN LAS EMPRESAS

REPUESTAS	*FRECUENCIA*	%
Muchas	6	16.67%
Pocas	2	5.56%
Muy Pocas	4	11.11%
Ninguna	24	66.67%
TOTAL	**36**	**100.00%**



ANALISIS

El 66.67% de los usuarios manifiestan que no poseen un manual de políticas de seguridad informática.

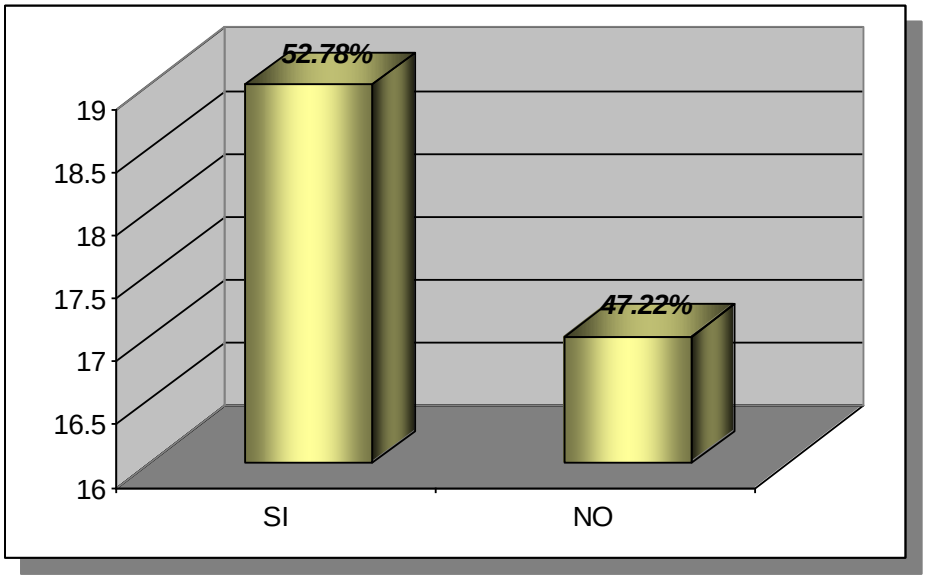
PREGUNTA No.6

¿Las personas que procesan y tienen acceso a la información contable, son exclusivamente del área contable?

OBJETIVO: Evaluar el cumplimiento de esta medida de Seguridad Informática en la entidad, e identificar un posible riesgo que la misma posea.

TABLA No.6
EXCLUSIVIDAD DEL PROCESAMIENTO ELECTRONICO DE DATOS POR USUARIOS DEL ÁREA DE CONTABILIDAD

REPUESTAS	*FRECUENCIA*	*%*
SI	19	52.78%
NO	17	47.22%
TOTAL	**36**	**100.00%**



ANALISIS

Se observa que un 80.56% de las personas que procesan la información contable pertenece al área contable, y que el 19.44% no pertenece a dicha área, lo cual incrementa el riesgo de que se realicen registros equivocados.

PREGUNTA No.7

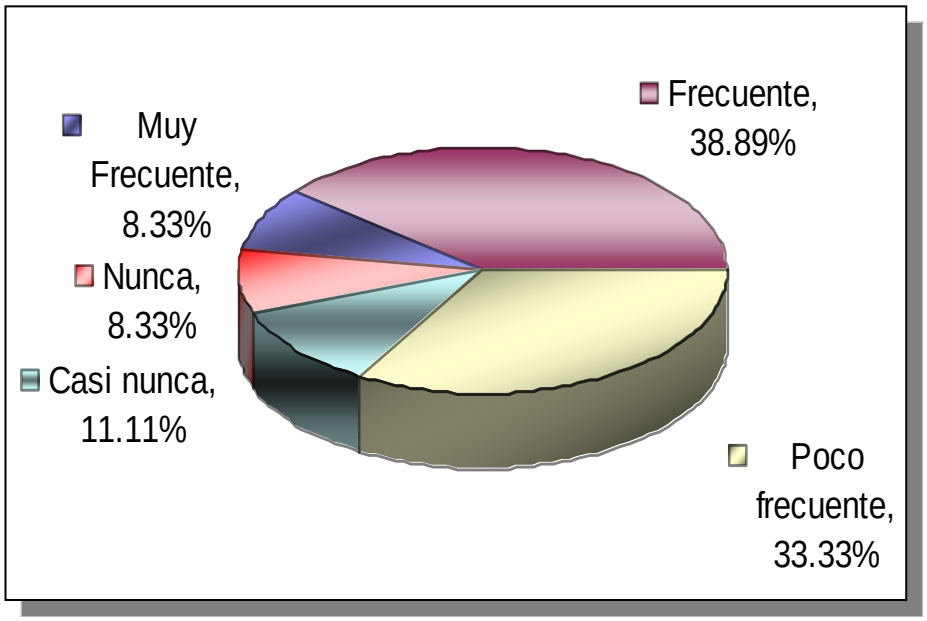
¿Con qué frecuencia ha observado perdidas de información contable?

OBJETIVO: Verificar si en las medianas empresas existe el riesgo de perdida de información y cuál es la frecuencia de ocurrencia de dicho evento.

TABLA No.7

PERDIDA DE INFORMACION CONTABLE

REPUESTAS	*FRECUENCIA*	%
Muy Frecuente	3	8.33%
Frecuente	14	38.89%
Poco frecuente	12	33.33%
Casi nunca	4	11.11%
Nunca	3	8.33%
TOTAL	**36**	**100.00%**



ANALISIS

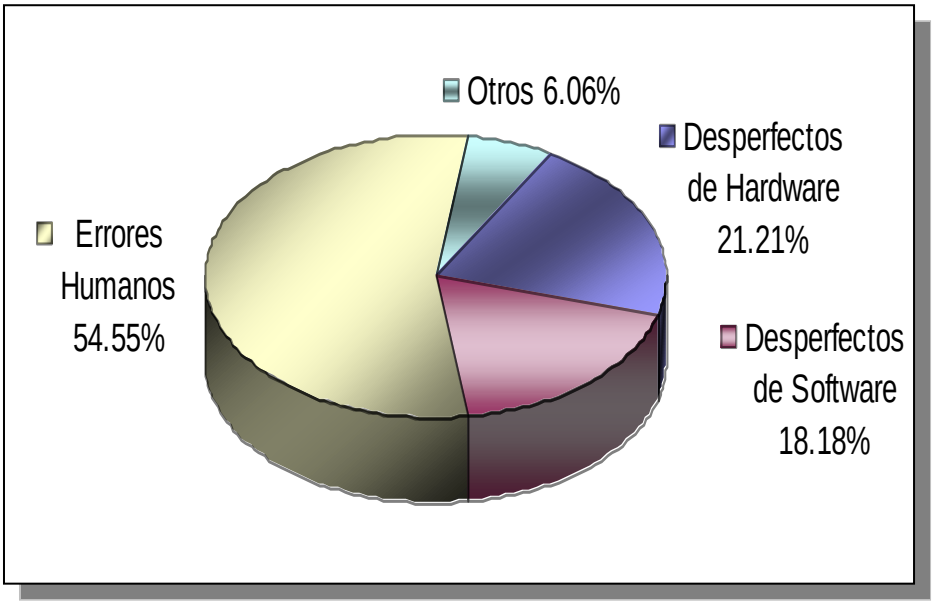
La pérdida de información dentro las empresas es de un 38.89% en la escala Frecuentes, opinando que se debe a la falta de procedimientos al registrar la información en los sistemas computarizados.

PREGUNTA 8
¿Cuál es la causa de las perdidas de información?

OBJETIVO: Determinar el origen de las perdidas de información en las medianas empresas.

TABLA No. 8
CAUSAS DE PERDIDA DE INFORMACION

REPUESTAS	*FRECUENCIA*	%
Desperfectos de hardware	7	21.21%
Desperfectos de software	6	18.18%
Errores humanos	18	54.55%
Otros	2	6.06%
TOTAL	**33**	**100.00%**



ANALISIS

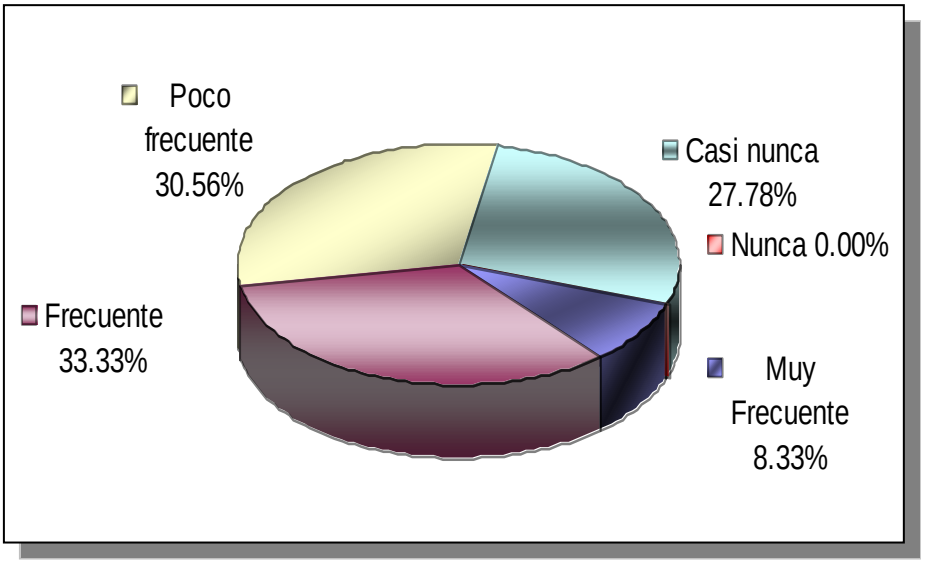
La perdida de información es ocasionada en un 54.55% por errores humanos, debido al desconocimiento del sistema, ocasionando así que se confunda y registre en forma errónea la información contable. Asimismo un 21.21% de la perdida es por errores del hardware.

PREGUNTA No.9
¿Con qué frecuencia ha tenido diferencias entre la información contable procesada electrónicamente y la información documental (física)?

OBJETIVO: Determinar la frecuencia con que existen diferencias entre la Información contable procesada electrónicamente y la documentación de soporte.

TABLA No.9
DIFERENCIAS ENTRE INFORMACION PROCESADA ELETRONICAMENTE VRS INFORMACION DOCUMENTAL

REPUESTAS	*FRECUENCIA*	*%*
Muy Frecuente	3	8.33%
Frecuente	12	33.33%
Poco frecuente	11	30.56%
Casi nunca	10	27.78%
Nunca	0	0.00%
TOTAL	**36**	**100.00%**



ANALISIS

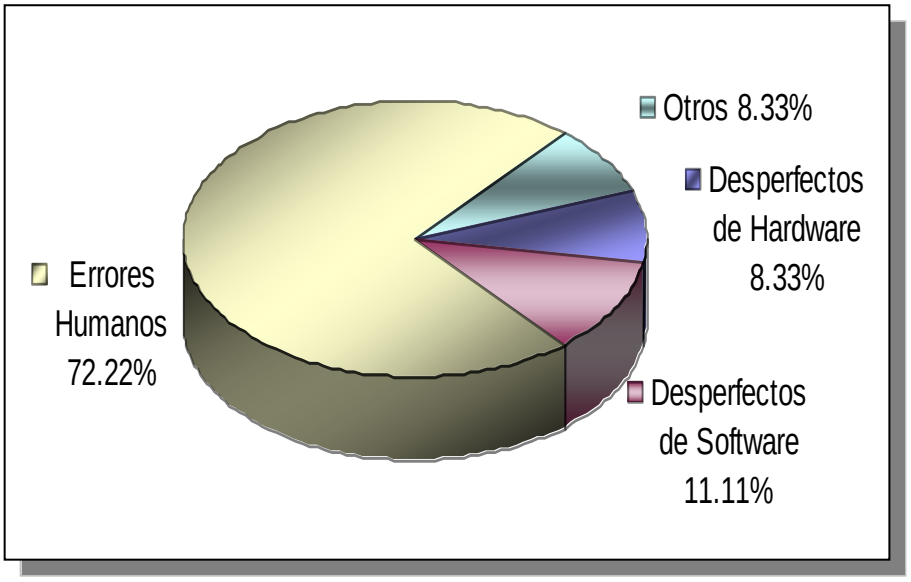
La existencia de diferencia de información en forma procesada electrónicamente y la documentación soporte es de 33.33%, aunque existe un 30.56% en el cual se manifiesta que las diferencias han sido poco frecuente, en ambos casos se confirma que en las empresas existe diferencia en la información contable.

PREGUNTA No.10
¿Cuáles son las causas de las diferencias entre la información con tablas procesada electrónicamente y la documental?

OBJETIVO: Determinar el origen de las diferencias en la documentación contable, y la considerar si en la empresa es vulnerable a un riesgo de Manipulación de Información.

TABLA No.10
CAUSAS DE DIFERENCIAS EN LA INFORMACION CONTABLES

REPUESTAS	*FRECUENCIA*	*%*
Desperfectos de hardware	3	8.33%
Desperfectos de software	4	11.11%
Errores humanos	26	72.22%
Otros	3	8.33%
TOTAL	**36**	**100.00%**



ANALISIS

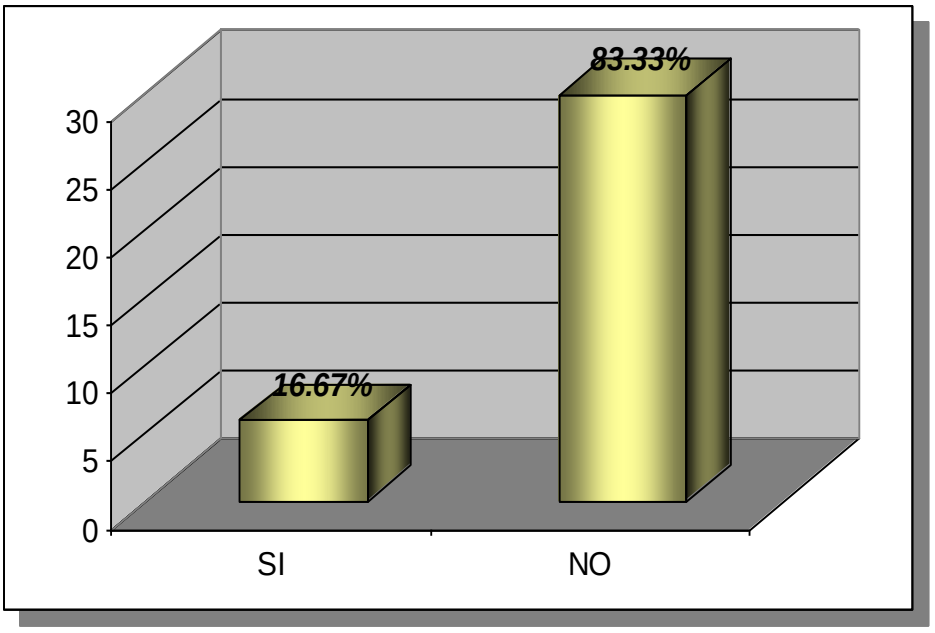
El desconocimiento del uso del sistema aunado al hecho de no poseer políticas que aseguren el procedimiento a seguir durante el registro de la información contable, ocasiona que en un 72.22% de la causa de diferencia en la información, sea por errores del usuario.

PREGUNTA No.11
¿Se ha dado alguna vez la divulgación de la información contable digital a personal no autorizado?

OBJETIVO: Considerar si la entidad implementa medidas para salvaguardar la información contable procesada electrónicamente.

TABLA No. 11
DIVULGACION DE INFORMACION CONTABLE DIGITAL
A PERSONAL NO AUTORIZADO

REPUESTAS	*FRECUENCIA*	*%*
SI	6	16.67%
NO	30	83.33%
TOTAL	**36**	**100.00%**



ANALISIS

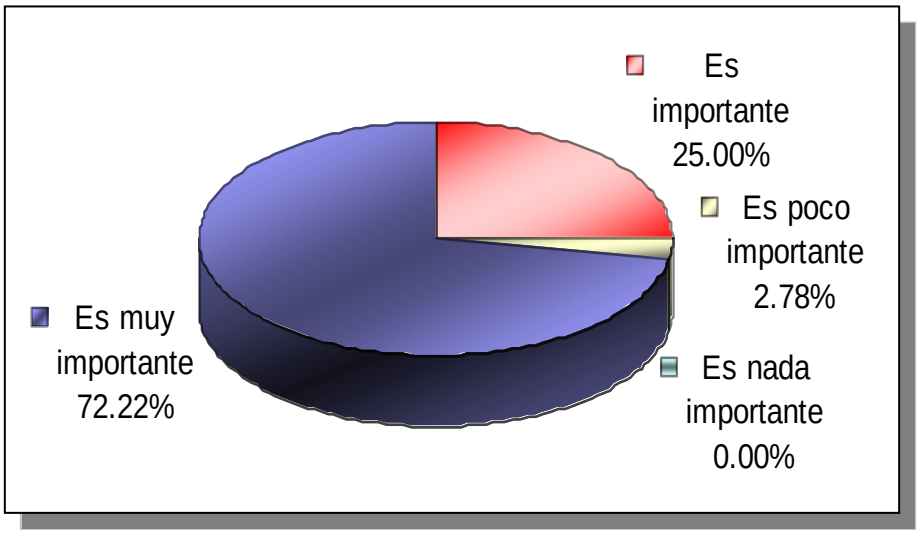
El 83.33% de los usuarios manifestaron que no existe divulgación a personal no autorizado sobre la información contable mientras que el 16.67% menciono que en alguna ocasión se ha permitido que personas ajenas al área tengan acceso a la información.

PREGUNTA No.12
¿Qué tan importante cree que es tener un Manual de políticas de seguridad informática para el procesamiento electrónico de datos?

OBJETIVO: Determinar la importancia que los usuarios estiman sobre la existencia de un Manual de Políticas de Seguridad Informática aplicable en el PED.

TABLA No.12
IMPORTANCIA DE UN MANUAL DE POLITICAS DE SEGURIDAD INFORMATICA PARA EL PED

REPUESTAS	*FRECUENCIA*	%
Es muy importante	26	72.22%
Es importante	9	25.00%
Es poco importante	1	2.78%
Es nada importante		0.00%
TOTAL	**36**	**100.00%**



ANALISIS

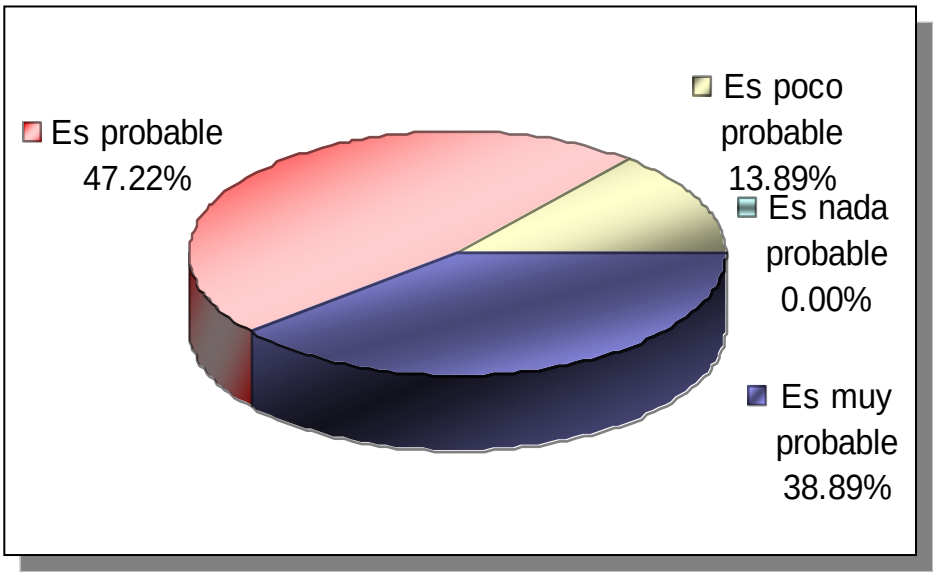
El 71.43% de los usuarios consideran que la existencia de un manual de políticas de seguridad informática es muy importante, ya que ayudaría a mejorar los procedimientos y evitar los errores que existen al momento de Procesar la información contable.

PREGUNTA No.13
¿Cree que el no poseer un Manual de Políticas de seguridad informática contribuye e a que se de una manipulación indebida de la información contable?

OBJETIVO: Considerar si los usuarios estiman que la existencia de un Manual de Políticas de Seguridad Informática para el PED, contribuiría a minimizar los riesgos de manipulación de la información contable.

TABLA No.13
OPINION DE LOS USUARIOS SI LA IMPLEMENTACION DEL MANUAL DISMINUIRA LA MANIPULACION DE INFORMACION CONTABLE

REPUESTAS	*FRECUENCIA*	*%*
Es muy probable	14	38.89%
Es probable	17	47.22%
Es poco probable	5	13.89%
Es nada probable	0	0.00%
TOTAL	**36**	**100.00%**



ANALISIS

Los usuarios opinan en un 47.22% que el no poseer un Manual de seguridad informática contribuye a que exista una manipulación indebida de la información contable.

PREGUNTA No.14
¿Por qué le gustaría implementar un Manual de Políticas de Seguridad Informática?

OBJETIVO: Determinar el nivel de aceptación y aplicación que el Manual de Políticas de Seguridad Informática obtendría entre los usuarios que procesan información contable en sistemas computarizados en las medianas empresas del sector comercio.

TABLA No.14
BENEFICIOS DEL MANUAL DE POLITICAS DE SEGURIDAD INFORMATICA

REPUESTAS	*FRECUENCIA*
Control interno	11
Integridad de la Información	3
Perdida de Información	9
Maximización de recursos	5
N/R	8

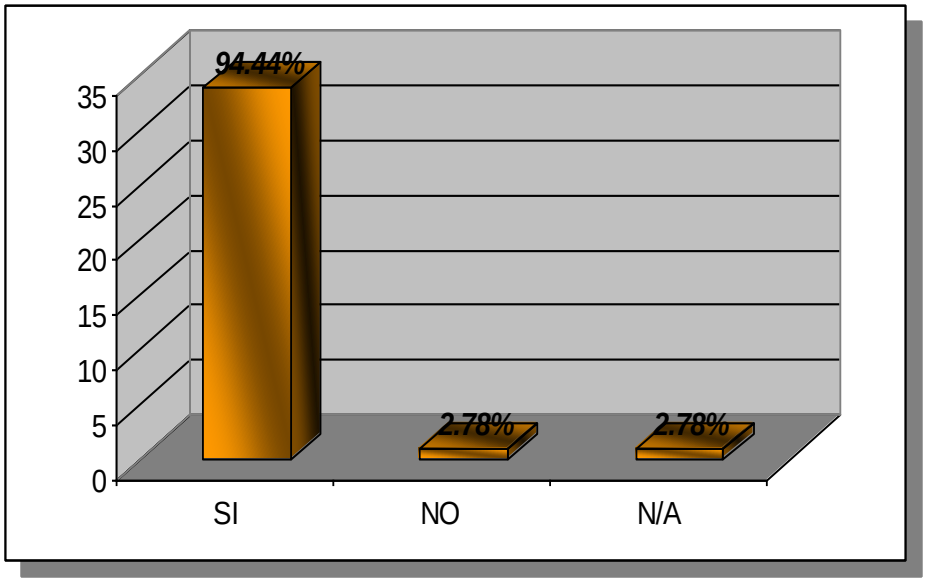
ANALISIS:
Entre los beneficios de implementar un manual de políticas de seguridad informática, se menciona que los mismos proporcionan una herramienta de control interno que educa al personal sobre la administración de los equipos informáticos y sobre el uso de los sistemas computarizados y la adecuada segregación de funciones. Asimismo disminuye el riesgo de perdida de información por medio de medidas para salvaguardar la misma; garantizando la integridad de la información procesada y contribuye a que se usen eficientemente los recursos de la empresa.

PREGUNTA No. 14
¿Estarían dispuestos a implementar un manual de políticas de seguridad informática?

OBJETIVO: Determinar el nivel de aceptación y aplicación que el Manual de Políticas de Seguridad Informática entre los usuarios que procesan información contable en sistemas computarizados en las medianas empresas del sector comercio.

TABLA No.13
ACEPTACION DE UN MANUAL DE POLITICAS DE SEGURIDAD INFORMATICA

REPUESTAS	*FRECUENCIA*	*%*
SI	34	94.44%
NO	1	2.78%
N/A	1	2.78%
TOTAL	**36**	**97.22%**



ANALISIS

La implementación de un Manual de Políticas de Seguridad Informática fuera aceptado en 94.44% dentro de las empresas, ayudando de esta manera a mejorar el proceso computarizado de datos contables.

PREGUNTA No.15
Mencione 5 políticas que usted considera que se debe incorporar en un Manual de seguridad informática.

OBJETIVO: Obtener un valor agregado proporcionado por los usuarios que procesan la información contable en las empresas, identificando las necesidades y áreas de importancia en el PED

TABLA No 15
POLITICAS CONSIDERADAS PARA INCLUIR EN UN MANUAL DE SEGURIDAD INFORMATICA.

REPUESTAS	*FRECUENCIA*	*%*
Back up	26	33.33%
Claves de acceso	20	25.64%
Adquisición y mantenimiento de antivirus	15	19.24%
Adecuada segregación de Funciones	11	14.10%
Uso de servidores	6	7.69%
TOTAL	**78**	**100.00%**

ANALISIS

Las políticas que los encuestados proponen para incluir dentro de un manual, son las que ellos conocen e implementan en su labor diaria, por lo cual es necesario incluir muchas políticas que no son aplicadas, para darle el valor agregado a la investigación.

2.2.2.Diagnostico

Los usuarios que hacen uso de sistemas informáticos en el PED, tienen conocimiento del término seguridad informática, aunque el estudio realizado comprobó que las empresas no poseen políticas, lo cual causa que la información procesada no sea integra, debido que aunque existen algunos procedimientos y controles aplicados a dicha actividad, los mismos no se implementan; pues la mayoría de los sistemas son adquiridos de forma empírica y además de la falta de políticas en el área.

En muy pocos casos, la existencia de políticas se encuentra detallada en forma verbal e informal, lo cual trae como consecuencia los errores humanos, convirtiéndose en la mayor causa para que se de la presentación errónea de la información contable. Otra de las causas que contribuyen a que se dé la pérdida y manipulación de la información es la no implementan medidas de seguridad que resguarden los equipos de cómputo, puesto que las empresas no cuentan con programas de mantenimiento de hardware, locaciones adecuadas del equipo para obtener un optimo rendimiento, porque se consideran como medidas innecesarias y costos adicionales a la empresa.

Lo anterior ocasiona desperfectos en el equipo y eso con lleva a que aumente el riesgo de pérdida de información y/o diferencia

entre la misma; invirtiendo más recursos en la reconstrucción de desperfectos en el software por mal funcionamiento en el hardware, además del tiempo que se emplea en recuperar la información pérdida.

Por lo cual la implementación de un manual de políticas de seguridad informática para el PED, representa un aporte que contribuirá a disminuir los riesgos inherentes a la manipulación de la información, ya que se comprobó la no existencia de dicho instrumento en las empresas en estudio y la disponibilidad de incorporarlo a sus actividades.

CAPITULO III

MANUAL DE POLITICAS DE SEGURIDAD INFORMATICA PARA EL PROCESAMIENTO ELECTRONICO DE DATOS CONTABLES

INDICE

I. INTRODUCION

En la Actualidad las organizaciones son cada vez más dependientes de los recursos informáticos que poseen, ya que proporcionan un importante beneficio en el desempeño de las operaciones de la entidad y permiten que el procesamiento electrónico de datos contables se efectué en forma ágil y eficiente.

Las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a cada uno de sus miembros, sobre la importancia y la sensibilidad de la información; en el alcance de las mismas existen diferentes aspectos a considerar entre los que podemos identificar tres grandes grupos que son la Seguridad Física, Lógica y de Redes.

La seguridad física incorpora los aspectos orientados a la parte tangible de la computadora y su entorno. La seguridad lógica incluye el control, manipulación, y accesos al sistema operativo y programas. La seguridad en redes incluye los accesos al servidor, comunicación y distribución de la información procesadas en las diferentes terminales de la entidad, además de la definición de los diferentes protocolos de seguridad.

El Alcance de estos tres aspectos se proporciona a través de políticas, que contribuyan a capacitar a los usuarios en medidas de seguridad informática, proporcionando un documento escrito para dicho fin.

Las políticas contenidas en este manual están compuestas por un objetivo, en el cual se estipula lo que se pretende lograr con la implementación de la política; un alcance que delimita el campo de acción en que se aplica la misma, un apartado de normas a seguir donde se brindan pautas que los usuarios deben considerar para llegar al objetivo planteado anteriormente; y finalmente los responsables, donde se mencionan los encargados del desarrollo, gestión e implementación.

II. OBJETIVO

a) Proporcionar una guía con políticas de seguridad informática que contribuya a minimizar el riesgo de manipulación de la información contable en las empresas, que sea de conocimiento y aplicación por los usuarios en el uso de recursos informáticos asignados en la entidad.
b) Estipular políticas de seguridad informática que puedan implementar los usuarios que procesan la información contable a través de recursos tecnológicos.

1. Seguridad Física.

1.1 Aseguramiento de las áreas

1.1.1 Aseguramiento del perímetro físico (ISO 17799 Num. 9.1.1/9.2.2/9.1.5; COBIT 4.0 dominio DS12.1)

POLITICA 1. Las paredes del perímetro deben estar hechas de materiales resistentes y que puedan prevenir en gran medida la contaminación del medio ambiente.

Objetivo: que los equipos de cómputo donde se procesa la información, se encuentren protegidos dentro de un cuarto definido y seguro.

Alcance: regulará la infraestructura del lugar donde se encontrarán los computadores.

Normas a seguir:

1. El material con que están hechas las paredes será de constitución resistente.
2. Las paredes deben encontrarse en buen estado.
3. El perímetro donde se guardan los equipos de cómputo no debe ser susceptibles a inundaciones u otra eventualidad de esa magnitud.
4. Al pasar algún desastre natural, la gerencia administrativa y los usuarios deben evaluar si el perímetro aun se considera seguro para las maquinas y los usuarios.
5. en caso de que el perímetro no esté seguro, comunicarlo lo antes posible a la gerencia administrativa.

Responsables del desarrollo, implantación y gestión: la implantación se hará por medio de órdenes, que deben ser giradas por la gerencia administrativa, los responsables de la implantación y gestión es el personal de contabilidad.

POLITICA 2. El cuarto donde están los equipos de cómputos no debe estar cerca de lugares peligrosos.

Objetivo: que el entorno del lugar donde se tienen las computadoras, sea seguro.

Alcance: está política se encargará de regular que el ambiente que rodea al centro de cómputo sea seguro, tanto para las maquinas como para los usuarios.

Normas a seguir:

1. La gerencia administrativa evaluará el medio ambiente del perímetro, y su seguridad para el centro de cómputo y los usuarios del mismo.
2. En caso de que el entorno al perímetro del centro de cómputo se vuelva inseguro, se deberá notificar a la gerencia administrativa para su pronto traslado.

Responsables del desarrollo, implantación y gestión: la implantación se hará por la gerencia administrativa, el cual velará junto con los usuarios, el monitoreo del entorno del centro cómputo.

1.1.2 Controles físicos de la entrada (ISO 17799 Num. 9.1.2; COBIT 4.0 dominio DS12.3)

POLITICA 1: Restringir el acceso al área donde se procesa la información contable computarizada.

Objetivo: que solo las personas encargadas de obtener, procesar y utilizar la información contable tengan acceso a esta.

Alcance: se regulará el acceso al personal en las áreas donde se procese la información contable y al centro de cómputo.

Normas a seguir:

1. Las personas que entran a suministrar la información al área de contabilidad no deberán permanecer por más de 5 minutos.
2. Identificar al personal de contabilidad por medio de gafetes, en el cual consignará su nombre y cargo.
3. En caso de que sea necesario el ingreso de personal no autorizado al lugar donde se procesa la información contable, por un período prolongado de tiempo, deberá ser vigilado por una persona autorizada.

Responsables del desarrollo, implantación y gestión: la implantación se hará por medio de órdenes, que deben ser giradas por la gerencia administrativa a los involucrados, los responsables de la implantación y gestión es el personal de contabilidad.

POLITICA 2. Tener una bitácora donde se detallen las personas que ingresan al centro de cómputo y bodegas.

Objetivo: llevar un control de la gente que entra y sale, en el lugar donde se procesa los datos contables.

Alcance: esta política regulara la afluencia de persona dentro del lugar donde se procesa la información contable.

Normas a seguir:

1. Debe haber una persona encargada de llevar el registro (bitácora) de las personas que entran y salen del departamento de contabilidad.
2. En la bitácora se deberá consignar la hora de llegada y la hora de retirada, además deberá colocar un detalle de la documentación entregada al visitante, en caso de que sea necesario.
3. Las personas no autorizadas, que quieran ingresar al departamento, deberán pedir a la gerencia administrativa que les otorgue el permiso respectivo y asignarle a la persona encargada de su vigilancia.
4. Queda prohibido el retiro de información contable, a personal que no sea de dicha área, sin previa autorización.
5. La gerencia administrativa es la encargada de proporcionar las autorizaciones escritas, para retirar documentos del área o despacho de contabilidad.

Responsables del desarrollo, implantación y gestión: el desarrollo y la implantación se hará por el departamento de contabilidad, y la gestión de esta política la hará la gerencia administrativa.

1.1.3 Aseguramiento de instalaciones
(ISO 17799 Num. 9.1.3; COBIT 4.0 dominios AI5.6/DS12.1)

POLITICA 1: Mantener una ventilación adecuada o con aire acondicionado en el cuarto donde se tienen los equipos informáticos.

Objetivo: mantener un sistema de enfriamiento o temperatura fresca los computadores, para que no presenten desperfectos.

Alcance: Dar pautas para mantener el equipo en buen estado y a una temperatura fresca.

Normas a seguir:

1. Mantener encendidos los aire acondicionado o mantener abiertas las ventanas (en caso de no tener aire acondicionado) para que haya una adecuada circulación de aire.
2. Mantener una temperatura adecuada, la temperatura que debe mantener el aire a acondicionado es de 23° a 25° centígrados.
3. En caso de no tener aire acondicionado, o que este no funcione, encender los computadores solo cuando sea necesario; en caso de continuar funcionando los mismos por periodos prolongados, darles descanso de una hora, para no sobrecalentar los equipos.
4. En caso de que el equipo sufra un recalentamiento, comunicarlo a al gerencia administrativa, para que tome las debidas medidas del caso.

Responsables del desarrollo, implantación y gestión: el responsable de la gestión es la gerencia administrativa, y los usuarios velaran por que la política se implante y se desarrolle de forma adecuada.

POLITICA 2. El lugar donde se van a instalar los computadores debe ser seguro.

Objetivo: Obtener la certeza de que el lugar donde se instalaran los computadores son seguros para estos.

Alcance: establecer pautas a tomar en cuenta para catalogar la seguridad del cuarto u oficina, donde se colocaran los computadores.

Normas a seguir:

1. Debe haber espacio suficiente para colocar, de forma adecuada, los computadores que se van a utilizar.
2. El lugar asignado para colocar los computadores no se debe encontrar cerca de lugares peligrosos (cerca de plantas de energía, campos magnéticos, deshechos químicos, etc.).
3. El lugar elegido debe ser seguro tanto para los computadores como para los usuarios.

Responsables del desarrollo, implantación y gestión: La gerencia administrativa es la responsable de la gestión e implantación de esta política, este se desarrollará por técnicos especializados, para evaluar el riesgo del lugar.

POLITICA 3. La empresa debe contar con instalaciones eléctricas adecuadas para la instalación de computadoras y sus periféricos.

Objetivo: Mantener una instalación eléctrica adecuada, para mantener los computadores y sus periféricos en perfecto estado.

Alcance: Dar las pautas a seguir para mantener una instalación eléctrica adecuada.

Normas a seguir:

1. Las instalaciones eléctricas deben poseer polo-tierra, para cualquier descarga eléctrica.

2. Tener un interruptor o térmico de emergencia, para cortar la energía cuando sea necesario.
3. Los interruptores de energía de emergencia se deben situar cerca de las salidas de emergencia, para facilitar el corte de energía.
4. Las líneas eléctricas deben poseer un voltaje adecuado, para poder trabajar con los equipo y no sobrecargarlos.
5. Todas las conexiones deben estar aisladas, aseguradas y no hayan cables de electricidad sueltos.
6. No conectar muchos aparatos aun solo toma, para evitar una posible sobrecarga.
7. En caso de que un usuario logre visualizar algún peligro, en las instalaciones eléctricas, deberá notificarlo de forma inmediata a la gerencia administrativa.

Responsables del desarrollo, implantación y gestión: La gestión de esta política la realizará la gerencia administrativa, en conjunto con los usuarios; el responsable del desarrollo será un técnico electricista capacitado.

1.1.4 Aseguramiento externo y ambiental
(ISO 17799 Num. 9.1.4; COBIT 4.0 dominio DS12.4)

POLITICA 1. Mantener herramientas y equipos apropiados, para hacerle frente a desastres naturales y casos fortuitos.

Objetivo: Estar preparado ante posibles amenazas de desastres naturales y casos fortuitos.

Alcance: Dar las medidas a adoptar ante cualquier desastre natural o caso fortuito.

Normas a seguir:

1. Mantener un extintor de incendios (como mínimo) en el área de cómputo.
2. Informar y capacitar a los usuarios sobre el uso de extintor.
3. Tener salidas de emergencia, para poder evacuar en caso de desastres naturales o casos fortuitos.
4. No mantener objetos colgados en el techo, como ventiladores, lámparas, etc.
5. Mantener los respaldos o back ups en cajas fuertes, dichas cajas deben estar diseñadas para soportar desastres naturales o casos fortuitos.
6. Mantener cámaras de monitoreo constante, tanto en el área de cómputo, como en el área donde se almacena la información y en sus alrededores.

Responsables del desarrollo, implantación y gestión: La gerencia administrativa será la encargada de la gestión y los técnicos especializados serán los encargados de capacitar a los usuarios.

POLITICA 2. Tener planes de contingencia para responder a desastres naturales y casos fortuitos.

Objetivo: Poseer un plan de contingencias operativo luego que haya sucedido un desastre natural o caso fortuito.

Alcance: Que cada uno de los usuarios conozca que procesos seguir, como respuesta ante un desastre natural o caso fortuito.

Normas a seguir:

1. Hacer un recuento de los daños materiales que ha quedado después de la eventualidad.
2. Evaluar que equipos o sus partes quedan en buen estado.
3. Evaluar las condiciones en que quedaron las instalaciones, para ver si se pueden reparar.
4. Hacer las reparaciones necesarias para reestablecer las instalaciones, y que estas estén aptas para poder rehabilitar el centro de cómputo.
5. Dejar la remoción de escombros, evaluación de daños y la reparación del local a personal técnico capacitado.
6. Verificar que la información almacenada en los computadores aun se puede rescatar.
7. Realizar un presupuesto de los equipos necesario para reestablecer el centro de cómputo.
8. Ya instalado el centro de computo, se procederá a cargar los back ups o respaldos de la información que sea necesaria.

Responsables del desarrollo, implantación y gestión: La gerencia administrativa, en conjunto con los usuarios, deberán gestionar la realización de esta política y el desarrollo será llevado a cabo por personal técnico capacitado, en desastres naturales y casos fortuitos.

1.1.5 Aseguramiento del área de entrega de información

(ISO 17799 Num. 9.1.5; COBIT 4.0 dominio DS12.2*)*

POLITICA 1. La información contable únicamente se retirará con previa autorización de la gerencia administrativa o delegado del área contable

Objetivo: prevenir la pérdida o la divulgación de la información procesada.

Alcance: Delimitar pasos a seguir para sacar la información fuera de las instalaciones donde esta es procesada.

Normas a seguir:

1. Informar a la gerencia administrativa o jefe delegado del área contable sobre la necesidad de sacar la información de donde se procesa.
2. Mantener una bitácora de la información que sale, describiendo en esta bitácora el día, la hora de entrada y salida, la persona que retira la información y el destino que tendrá dicha información.
3. La información deberá regresarse a su lugar de almacenamiento en el lapso de una semana, solo por exigencias de la gerencia administrativa este plazo se podrá prorrogar.
4. En caso de que la información sea exigida por entes externos de la empresa, se pedirá una autorización escrita a la gerencia administrativa.
5. Dar copias a personas extrañas al departamento de contabilidad, en caso de tratarse de instituciones gubernamentales, deberá sacarse fotocopia a los documentos originales entregados, consignando en la copia el nombre, dependencia estatal que proviene, la fecha de entrega y la firma del funcionario (además de consignar una copia de la debida identificación del funcionario).

Responsables del desarrollo, implantación y gestión: La gestión y el desarrollo de está política estará a cargo de los usuarios, ya que ellos son responsables de la información procesada y proporcionada.

1,2 Seguridad del equipo

1.2.1 Localización y protección
(ISO 17799 Num. 11/9.2.1; COBIT 4.0 dominio DS12.5)

POLITICA 1: Los equipos de cómputo y los medios de almacenamiento físicos deben estar ubicados adecuadamente.

Objetivo: mantener en un lugar seguro los equipos de computo y las copias de seguridad (back ups) realizados.

Alcance: regular donde debe estar el equipo de cómputo, así como proporcionar normas a implementar para mantener resguardado el hardware y los medios de almacenamiento de los back ups.

Normas a seguir:

a) Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de garantía de los mismos sin la autorización de la dirección de administrativa, en caso de requerir este servicio deberá solicitarlo a los técnicos encargados del mantenimiento.
b) Los computadores deben ser colocados en un ángulo de visión restringido, para reducir el riesgo de que la información sea vista por personal desautorizado.
c) El equipo informático se ubicara en un entorno limpio y sin humedad.
d) Los cables de conexión no deben ser pisados, cortados o pinchados.
e) No se colocaran objetos sobre los cables de conexión.

f) Notificar con una semana de anticipación, a la dirección general administrativa, los cambios o reubicaciones de los computadores.

Responsables del desarrollo, implantación y gestión: los responsables de desarrollar estas políticas son los usuarios del centro de cómputo; la implantación estará a cargo de la dirección general administrativa.

POLITICA 2: Los equipos de cómputo y los medios de almacenamiento físicos deben estar resguardados.

Objetivo: Resguardar los equipos de computo y las copias de seguridad (back ups) realizados.

Alcance: Que los usuarios implementen normas, para proteger y mantener en buenas condiciones el hardware, medios de almacenamiento y back ups.

Normas a seguir:

1. El usuario tiene la obligación de proteger los discos, disquetes, cintas magnéticas y CD-ROM que se encuentren bajo su administración, aún cuando no se utilicen y contengan información reservada o confidencial.
2. No consumir alimentos o ingerir líquidos mientras se opera el equipo de cómputo.
3. No colocar objetos sobre el equipo y/o cubrir los orificios de ventilación del monitor o del CPU.
4. Los usuarios no deben abrir o desarmar los equipos de cómputo.
5. Los artículos o periféricos y unidades de almacenamiento que requieren la protección especial, se deben aislar para

reducir el nivel general de protección requerida (como diskette, CD-Rom, Memorias USB, etc.).

Responsables del desarrollo, implantación y gestión: los responsables de desarrollar estas políticas son los usuarios del centro de cómputo; la implantación estará a cargo de la dirección general administrativa.

POLITICA 3: El equipo debe de protegerse contra cambios en el voltaje o corte de energía eléctrica.

Objetivo: Resguardar los equipos de computo contra cualquier corte de energía o cambios en el voltaje.

Alcance: establecer lineamientos a seguir para proteger el equipo contra corte de energía o cualquier otra interrupción.

Normas a seguir:

1. Cada computador contará con una fuente de alimentación continua (UPS), para que los equipos y sus periféricos no sufran desperfectos por cambios de voltaje o falta del suministro de energía eléctrica.
2. Mantener un generador de reserva, para que los equipos sigan funcionando en un corte de energía prolongado y evitar suspender las operaciones de la entidad.
3. Mantener mucho combustible, el cual debe estar disponible para asegurarse de que el generador pueda estar en función por un período prolongado.
4. El equipo y los generadores (UPS) se deben comprobar regularmente, para asegurarse tiene capacidad adecuada y probarse de acuerdo con las recomendaciones del fabricante.

Responsables del desarrollo, implantación y gestión: los encargados de la implantación y el desarrollo son los usuarios, la gestión la realizará la gerencia administrativa.

1.2.2 Mantenimiento y Reparación
(COBIT 4.0 dominio DS13.5)

POLITICA 1: Los Equipos de cómputo y sus periféricos tendrán mantenimiento Preventivo regularmente.

Objetivo: Mantener los computadores y sus periféricos en optimas condiciones para realizar el trabajo cotidiano.

Alcance: Dar lineamientos a seguir para proporcionar mantenimiento adecuado a los computadores y sus periféricos.

Normas a seguir:

1. El mantenimiento de los equipos de cómputo y sus periféricos debe efectuarse de forma periódica (por lo menos cada 3 meses).
2. El mantenimiento de los computadores y sus periféricos será realizado por personal técnico capacitado, el cual será designado por la gerencia administrativa.
3. Esta prohibido que los usuarios le den el mantenimiento a los equipos de cómputo y sus periféricos.
4. Cada usuario será orientado por personal técnico especializado sobre como limpiar la parte exterior de los computadores y sus periféricos.
5. El técnico designado para dar mantenimiento a los computadores y sus periféricos debe de poseer un historial de las averías.
6. Toda documento de garantía del equipo se mantendrá en un lugar seguro, hasta su vencimiento, y tomar en cuenta las

cláusulas contenidas en este al momento de dar el mantenimiento.

7. En caso de tenerse asegurados los equipos y sus periféricos, las pólizas de seguro se deberán mantener en un lugar seguro.

Responsables del desarrollo, implantación y gestión: los usuarios y la gerencia administrativa son los encargados de gestionar esta política, y los encargados del desarrollo son los técnicos capacitados, designados por la gerencia administrativa.

POLITICA 2: Las líneas de energía y telecomunicaciones deben ser subterráneas o no estar al alcance de los usuarios o terceros.

Objetivo: Proteger los cables de energía y telecomunicaciones, de cualquier tipo de daño.

Alcance: Normar el ordenamiento de las instalaciones y de líneas de energía y telecomunicaciones.

Normas a seguir:

1. los cables de energía y de telecomunicaciones se encontraran fuera del alcance de los usuarios
2. No quitar, mover o cortar los cables de energía y telecomunicaciones.
3. Los técnicos especializados y designados por la gerencia administrativa, son los encargados de la instalación, ordenamiento y reparación de los cables.
4. Si se detecta algún peligro potencial con respecto a los cables de energía o de telecomunicaciones, comunicarlo de

inmediato a la gerencia administrativa, para su pronta solución.

Responsables del desarrollo, implantación y gestión: los usuarios y la gerencia administrativa son los encargados de gestionar esta política, y los encargados del desarrollo son los técnicos capacitados, designados por la gerencia administrativa.

POLITICA 3: La reparación de equipos de cómputos y periféricos lo realizara el personal técnico capacitado.

Objetivo: delimita quienes están a cargo del la reparación del hardware, por cualquier tipo de desperfectos.

Alcance: esta política es aplicable para los usuarios de los equipos de cómputo y los técnicos capacitados.

Normas a seguir:

1. Notificarse inmediatamente cualquier desperfecto que tenga el computador y/o sus periféricos.
2. Los técnicos son responsables de arreglar cualquier desperfecto en los computadores.
3. Los técnicos serán designados por la gerencia administrativa.
4. Los técnicos deberán revisar el equipo y dar un informe a la gerencia administrativa, para que este pueda decidir el curso de acción a seguir, en la asignación de tareas.

Responsables del desarrollo, implantación y gestión: los responsables de ejecutar esta política son los técnicos, los cuales pueden ser de la propia compañía o sub-contratados.

POLITICA 4: Mantener equipos de cómputo de reserva, para cuando uno o más de los equipos estén en reparación.

Objetivo: que el procesamiento electrónico de datos no se afecte por la falta del equipo de cómputo.

Alcance: dar las pautas a seguir por los usuarios, cuando un equipo de cómputo está en reparación.

Normas a seguir:

1. Mantener un equipo de cómputo disponible, mientras uno se encuentre en reparación, para que se utilice por los usuarios.
2. En que caso de que dos o más equipos estén en reparación, deberán implementar un cronograma de usos de las computadoras en funcionamiento, entre todos los usuarios.

Responsables del desarrollo, implantación y gestión: los encargados de asignación del equipo de disponible y realización del cronograma de uso es la gerencia administrativa, los cuales deben ser acatados por los usuarios.

1.2.3 Disposición y reutilización
(ISO 17799 Num. 9.2.6; COBIT 4.0 dominio DS12.2)

POLITICA 1: Siempre revisar los medios de almacenamiento en desuso y la información almacenada en ellos, antes de ser desechados o reutilizados.

Objetivo: Mantener medios de almacenamiento disponibles y evitar la divulgación no autorizada de información.

Alcance: normar las formas de revisión de los medios de almacenamiento físico, y dar el tratamiento aplicable a los medios de almacenamiento defectuosos

Normas a seguir:

1. Que los medios de almacenamiento que se encuentren en buen estado sean formateados y reutilizados.
2. Verificar que tipo de información contiene los medios de almacenamiento, y si esta puede ser objeto de recuperarse.
3. Borrar la información que se tenga duplicada, de forma segura y adecuada, y reutilizar el medio de almacenamiento.
4. En caso que el medio de almacenaje ya no funcione correctamente, se procederá a la destrucción, para evitar la divulgación de información

Responsables del desarrollo, implantación y gestión: los responsables de ejecutar esta política son los usuarios, el cual será gestionada por la gerencia administrativa.

1.2.4 Retiro y manejo.
(ISO 17799 Num. 9.2.5/ 9.2.7; COBIT 4.0 dominio DS12.2)

POLITICA 1: Las partes en buen estado de los equipos y periféricos que se retiran, podrán ser utilizadas con autorización en otros.

Objetivo: reutilizar partes de los equipos y sus periféricos, y así evitar gastos innecesarios para la empresa.

Alcance: establecer los pasos a realizar, para desechar un computador, una parte del computador y sus periféricos.

Normas a seguir:

1. Verificar que el estado en que se encuentran el computador, sus partes y sus periféricos.
2. Si varias partes de un computador retirado se encuentran en buen estado, evaluar conforme a las necesidades de los equipos su incorporación en los mismos.
3. Instalar las partes en buen estado en los computadores que las requieran.
4. Retirar y desechar los componentes inservibles.
5. Solo los técnicos especializados tiene la autorización para revisar, evaluar y retirar los equipos, partes y sus periféricos.

Responsables del desarrollo, implantación y gestión: los responsables de ejecutar esta política son los Usuario, el cual será gestionada por la gerencia administrativa.

2. Seguridad Lógica

2.1.Validación en acceso a software.

2.1.1 Identificación y autentificación de usuario
(ISO 17799 Num. 11.5.2; COBIT 4.0 dominios DS5.3/DS5.4)

POLITICA 1. Cada usuario debe de tener su identificación en su computador.

Objetivo: prevenir el ingreso de usuarios no autorizados dentro del sistema informático.

Alcance: identificar que usuarios son los autorizados para tener acceso al sistema informático.

Normas a seguir:

1. Cada uno de los usuarios poseerá un identificador único (ID).
2. La creación de los ID deberán ser por medio de un formulario.
3. Ninguna ID deberá repetirse.
4. Se llevará un registro detallado de cada uno de los usuarios existentes.
5. En ningún momento el usuario debe de prestar, divulgar o mencionar, su ID a ningún otro usuario (interno o externo)
6. Las ID que estén cerradas no se asignarán a ningún otro usuario, las mismas se considerarán para el historial correspondiente.
7. Se le deberá de explicar a los usuarios las responsabilidades y normas que posee la administración sobre el uso adecuado de las ID.

Responsables del desarrollo, implantación y gestión:

1. El Supervisor de cada área, será el responsable de solicitar la creación de las ID para los usuarios que tenga a su cargo.
2. El formulario deberá de ser firmado por el supervisor ó jefe de cada departamento, además de ser firmado por el usuario correspondiente.
3. Solo el usuario maestro debe ser el responsable de la creación de las ID.
4. El usuario maestro deberá llevar el registro de cada uno de las ID activas como las ID inactivas, en ningún momento se deberá de divulgar dicha información sin la autorización de la administración.
5. Cuando un usuario sea despedido, el supervisor o jefe de área deberá de informar al usuario maestro para que la ID

de dicho usuario sea bloqueada para que no se pueda utilizar mas.

6. Si el usuario divulga, menciona, o presta su ID a otro usuario se sancionara por la administración.

POLITICA 2. Cada usuario debe tener su propia clave de acceso.

Objetivo: Conocer y determinar el uso que los usuarios autorizados hacen del sistema informático.

Alcance: Que la identidad del usuario pueda ser verificada correctamente.

Normas a seguir:

1. Para cada una de las ID, se asignará una clave de acceso.
2. Las claves de acceso deberán de funcionar para la ID correspondiente, en ningún caso deberá de funcionar con otras ID.
3. La clave deberá de ser memorizada inmediatamente, no se deberán anotar.
4. La clave de acceso deberá de contener no menos de cinco dígitos, permitiendo el uso de rangos alfanuméricos, símbolos, y permitir la combinación de Mayúsculas y Minúsculas.
5. Al ingresar incorrectamente la clave de acceso, después de 3 intentos, se deberá de bloquear la ID para evitar la manipulación de información.
6. Para las ID bloqueadas deberán de solicitarse una ID provisional que permita al usuario accesar a la ID para asignar una nueva clave de acceso.
7. El usuario en ningún momento deberá de divulgar, mencionar o prestar su clave de acceso a otro usuario (interno o externos).

8. El cambio de clave será cada 90 días.

Responsables del desarrollo, implantación y gestión:

1. Con la creación de las ID, se deberán de crear la clave de acceso que deberá de conocer solo el usuario.
2. El usuario maestro deberá de supervisar que la clave establecida no funcione con otro usuario dentro del sistema.
3. Cuando la clave sea olvidada o extraviada se deberá de informar al supervisar y este le informara al usuario maestro, para que asigne una clave provisional que permita al usuario entrar al sistema y reasignarse la contraseña.
4. El usuario maestro deberá de programar el sistema para que cada 90 días se cambie la clave de acceso.

2.1.2 Temporalización de la sesión (ISO 17799 Num. 11.5.5; COBIT 4.0 dominios DS5.2/DS5.4)

POLITICA 1. Las sesiones de los usuarios deben bloquearse en un período determinado de tiempo.

Objetivo: que las sesiones que estén inactivas deberán cerrarse después de 5 minutos o definir un tiempo determinado.

Alcance: El evitar que la información sea manipulada mientras el usuario no se encuentra.

Normas a seguir:

1. Después de cinco minutos que el sistema este como inactivo se deberá de bloquear la pantalla evitando el acceso desautorizado a dicho sistema.

2. Siempre que el usuario se levante de su puesto deberá de dejar bloqueada su maquina y desbloquearla cuando regrese a su área de trabajo.
3. El desbloqueo deberá de ser por medio de las clave de acceso del ID que se encuentre en actividad.
4. Si la ID ya no se mantendrá activa, se deberá cerrar la sesión.

Responsables del desarrollo, implantación y gestión:

1. El usuario será el responsable de que la ID quede bloqueada mientras no se encuentre trabajando.
2. El supervisor debe verificar que el sistema quede bloqueado mientras el usuario no se encuentra.
3. El usuario maestro debe programar el sistema para que se realice la temporalización de la sesión después de los cinco minutos de inactividad.
4. El usuario maestro programará el sistema para que este reconozca la clave de acceso como la clave de desbloqueo.

2.1.3 Restricción de acceso de información (ISO 17799 Num. 11.6.1; COBIT 4.0 dominios DS5.2/DS11.3)

POLITICA 1. Solo el personal que procesa la información debe tener acceso a esta.

Objetivo: prevenir el acceso desautorizado a la información.

Alcance: Que los usuarios trabajen sin una supervisión minuciosa por parte de los supervisores.

Normas a seguir:

1. Identificar y delimitar cada una de las funciones, actividades o roles, que tendrá el usuario dentro de la entidad.
2. Según las funciones, actividades o roles, al usuario se le permitirá accesos como: Lectura, Escritura, Ejecución, Borrado, Creación y Búsqueda.
3. El sistema debe de realizar un log o registro de cada uno de los procedimientos realizados por el usuario.
4. El usuario solo podrá accesar a la información durante las horas establecidas por sus funciones, actividades o roles, asignados por la administración.
5. El sistema mandara un correo o llamado de alerta al usuario maestro informando el acceso al sistema después de horas asignadas al usuario.
6. Cada mes se realizará un análisis a cada una de las ID, determinando sus funciones y accesos respectivos.
7. Cuando ya no se requiera un acceso deberá de ser retirado de los derechos que posee la ID dentro del sistema.

Responsables del desarrollo, implantación y gestión:

1. El supervisor entregara un listado de cada una de las funciones que posee el usuario para que el usuario maestro le asigne los accesos necesarios para realizar su trabajo.
2. El usuario maestro informará cualquier acceso que no este autorizado.
3. El supervisor, el usuario maestro y el usuario deberán de realizar un análisis de las funciones y accesos que serán permitidos a las ID dentro del sistema.
4. El supervisor dejara por escrito la asignación de derechos que posea la ID, considerando si se aplica una incorporación o eliminación de derechos.

2.2.Mantenimiento del Software.

2.2.1 Controles contra códigos malévolos
(ISO 17799 Num. 10.4.1 y 10.4.2; COBIT 4.0 dominio DS5.9).

POLITICA 1. Se debe tener controles adecuados contra códigos malévolos.

Objetivo: Proteger la integridad del software y la información existente.

Alcance: realizar la detección, la prevención contra códigos malévolos que resguarden la información existente.

Normas a seguir:

1. Ningún usuario podrá instalar software que no este autorizado por la administración o el encargado de informática.
2. Se revisara en forma regular el contenido que posea el software y datos del sistema, verificando si existen códigos malévolos.
3. Eliminar cualquier software que no esté autorizado por la administración.
4. Se autorizaran e instalaran un sistema de protección legal que verifique la existencia de códigos malévolos dentro de la información entrante.
5. La verificación de la información será de forma automática una vez se reconozca el acceso y la existencia de códigos malévolos deberá de ser eliminado inmediatamente.
6. Se programara el sistema para que en el caso de que se desee instalar algún programa pirata sea denegada la petición si no tiene el permiso de la administración

Responsables del desarrollo, implantación y gestión:

1. La instalación del software para la protección de la información, será realizada por la administración y el usuario maestro.
2. El sistema de protección se programará por el usuario maestro.
3. El usuario maestro deberá instalar en cada maquina el programa de protección contra códigos malévolos.
4. regularmente realice una revisión completa al software para detectar la existencia de códigos malévolos.

2.2.2 Control de acceso al código fuente del programa.
(ISO 17799 Num. 12.4.3; COBIT 4.0 dominio DS5.2)

POLITICA 1. Tener controles adecuados para prevenir el acceso al código principal del programa.

Objetivo: Proteger el acceso al código fuente del programa.

Alcance: Evitar que se realicen cambios desautorizados en la funcionalidad del programa.

Normas a seguir:

1. El acceso al código fuente del sistema, estará completamente restringido a todo usuario no autorizado.
2. Los cambios al código fuente serán por medio de autorización y se realizaran para que el sistema funcione correctamente.
3. La documentación referente a los accesos que posee el sistema deberán de ser puestos en un lugar resguardado.

Responsables del desarrollo, implantación y gestión:

1. El acceso al código fuente será realizado solo por el usuario maestro, previa autorización de la administración.

2. La administración tendrá bajo su cuidado toda la documentación referente al sistema informático.

2.2.3 Mantenimiento de programas. (COBIT 4.0 dominio DS5.2)

POLITICA 1. Dar mantenimiento a correctivo y preventivo los sistemas informáticos contables.

Objetivo: Proteger y verificar la información existente dentro de los programas informáticos.

Alcance: Evitar la manipulación al sistema informático y a la información existente.

Normas a seguir:

1. Se verificara periódicamente el funcionamiento de los sistemas informáticos.
2. Se informara a los usuarios correspondientes las actualizaciones realizadas al sistema informático.
3. Se instalaran programas utilitarios que ayuden al mantenimiento de los sistemas informáticos.
4. Se realizaran actualizaciones al sistema informático periódicamente.
5. Se ejecutaran pruebas a las actualizaciones realizadas y se analizara las mejoras que ocasiona al usuario al momento de ejecutar sus operaciones o si las mismas no son adecuadas para el funcionamiento.

Responsables del desarrollo, implantación y gestión:

1. El usuario informara de la necesidad de realizar las actualizaciones al sistema informático a su supervisor para que notifique al usuario maestro.

2. Se realizaran pruebas a las actualizaciones por parte del usuario para que compruebe la eficiencia de las actualizaciones y compruebe su funcionalidad en el mejoramiento de las operaciones.
3. Quedaran sustentados por el usuario maestro las actualizaciones existentes.

2.2.4 Mantenimiento de los sistemas operativos. (COBIT 4.0 dominio DS5.2)

POLITICA 1. Dar mantenimiento correctivo y preventivo a los sistemas operativos existente.

Objetivo: Proteger y verificar el funcionamiento del sistema operativo.

Alcance: Evitar la generación de errores dentro del sistema operativo por falta de mantenimiento.

Normas a seguir:

1. Se verificara periódicamente el funcionamiento de los sistemas operativo en búsqueda de errores existentes.
2. Las actualizaciones se realizaran para el mejoramiento del sistema operativo, previniendo daños al sistema informático.
3. Se instalaran software utilitario que ayuden al mantenimiento del sistema operativo.
4. Se negara el acceso a las carpetas y configuración del sistema operativo para que se evite la manipulación de los archivos existentes.

Responsables del desarrollo, implantación y gestión:
Las actualizaciones al sistema operativo será realizada por el usuario maestro considerando que las mismas deberán de

permitir un mejor funcionamiento, evitando que el usuario tenga acceso a carpetas del sistema y ocasione perdidas de información y/o daños graves al equipo.

2.2.5 Uso de las utilidades de sistema (COBIT 4.0 dominio DS5.2)

POLITICA 1. Instalar programas utilitarios dentro del sistema.

Objetivo: Verificar que los programas utilitarios no afecten la ejecución del sistema informático y operativo.

Alcance: Prevenir las fallas en el sistema informático y operativo.

Normas a seguir:

1. La existencia de programas utilitarios serán evaluadas y utilizados de tal manera que permita el funcionamiento adecuado del sistema.
2. Se permitirá el acceso al usuario a los sistemas utilitarios para la realización de sus operaciones.
3. Verificar que los programas existentes no ocasionen fallos dentro de los sistemas informáticos y operativos.

Responsables del desarrollo, implantación y gestión:

1. El usuario informara al supervisor correspondiente para que verifique los sistemas que son necesarios para la ejecución de sus actividades.
2. El usuario maestro verificara que los programas utilitarios no ocasionen los controles del sistema operativo.
3. El usuario maestro será el que permita el acceso a programas utilitarios.

4. El usuario maestro realizara un análisis de los sistemas utilitarios que necesitara el usuario para realizar sus operaciones.

2.3. Procesamiento de la Información Contable.

2.3.1 Control del Proceso Interno (COBIT 4.0 dominio DS13.4)

POLITICA 1. Mantener un control interno adecuado para el procesamiento electrónico de datos contables.

Objetivo: Verificar la integridad de la información que será utilizada para el procesamiento electrónico de datos.

Alcance: Que la información sea ingresada adecuadamente por el departamento de contabilidad.

Normas a seguir:

1. La información será clasificada dependiendo de cada una de las áreas existentes dentro del departamento de contabilidad
2. Solo se ingresara información que esté debidamente respaldada.
3. Se anotara en la documentación la fecha en que fue entregada.
4. La documentación se ingresará de acuerdo al orden sistemático del programa contable.
5. Se realizara una verificación de la información procesada, asegurando que no halla duplicidad de la información.
6. La eliminación, la búsqueda de registro, será realizada por el usuario autorizado para hacerlo.
7. Se realizara un registro de cada uno de los procesamientos realizados durante el día, que identifique: día, mes, año, ID, y procesamiento que realizo.

Responsables del desarrollo, implantación y gestión:

1. El jefe del departamento de contabilidad verificara la información antes de ser entregada a los usuarios que realizaran el procesamiento de datos.
2. El usuario realizara una revisión previa a la documentación, evitando la duplicidad de datos.
3. Los cambios en el registro serán realizados por el usuario responsable (de preferencia deberá de ser el supervisor del área contable).
4. El usuario deberá de anotar en la documentación la fecha en que le es entregada por parte del supervisor o jefe de área.

2.3.2. Intercambio de la información contable.
(ISO 17799 Num. 10.8.1; COBIT 4.0 dominio DS5.11)

POLITICA 1. El intercambio de información contable deber ser de forma adecuada y a la persona que corresponda.

Objetivo: prevenir la recepción y manipulación de información por usuarios desautorizados.

Alcance: El intercambio de información será emitida por el departamento de contabilidad y será entrega a los usuarios autorizados.

Normas a seguir:

1. La administración debe identificar los usuarios autorizados que tendrán acceso a la información contable.
2. Se podrá enviar la información contable por medio de correo electrónico, memorias USB, pero únicamente a usuarios autorizados.

3. La información contable deberá ser cifrada por medio de archivos especiales que eviten que la misma sea visualizada por usuarios desautorizados.
4. Se deberá realizar un registro que detalle la información que ha sido entregada a los demás usuarios.

Responsables del desarrollo, implantación y gestión:

1. El Supervisor de cada área, informara a los usuarios que recibirán la información contable, que en ningún caso deberán entregar la misma, a otros usuarios sin previa autorización.
2. El reporte de entrega de información deberá de ser respaldada por la firma del jefe del departamento y por el supervisor de área, cuando el envió sea por medio de correo electrónico, se deberá de imprimir y deberá de ser agregado al informe.
3. Los archivos serán programados por el usuario maestro para que solo sean descifrados por el usuario que este autorizado para recibir la información.

2.3.3 Validación de datos de entrada
(ISO 17799 Num. 12.2.1; COBIT 4.0 dominio DS5.5)

POLITICA 1. Los datos contables ingresados durante el procesamiento electrónico deben ser validados.

Objetivo: Asegurar la veracidad de la información procesada dentro del sistema informático contable.

Alcance: identificar los errores existentes dentro del área de procesamiento electrónico de datos contables.

Normas a seguir:

1. Una vez procesada la información, se deberá realizar una verificación detallada de cada documentación procesada,

permitiendo que los datos estén de forma correcta y apropiada.

2. Cualquier error de cálculo, o ingreso incorrecto de datos debe ser reportado y corregido inmediatamente.
3. No se permitirá alterar periodos contables ya cerrados.
4. La verificación se hará de forma periódica, evitando que la información se de por finalizada de forma incorrecta.
5. Los errores deberán de ser detallados por medio de informe donde demuestre la ID del usuario responsable de procesarla.
6. Los errores atribuibles al software deberán ser reportados para adoptar las medidas necesarias.
7. Si los errores son encontrados después de que se finalice el periodo, el registro correcto deberá de ser informado durante el periodo actual, por medio de ajustes.

Responsables del desarrollo, implantación y gestión:

1. El Supervisor de cada área, deberá designar el personal que estará a cargo de la validación de la información.
2. El personal encargado deberá realizar la validación de forma periódica, de preferencia cada fin de semana.
3. La validación será utilizando la documentación física versus la documentación magnética, constatando la existencia de discrepancias.
4. Si el error es por parte del software se deberá de informar al usuario maestro para que realice las actualizaciones respectivas.
5. Si el error es por parte del usuario, se deberá de informar tanto al supervisor como al usuario, para evitar errores futuros.

2.3.4 Salida de la información contable
(ISO 17799 Numeral 12.5.4; COBIT 4.0 dominio DS13.4)

POLITICA 1. Se debe monitorear la salida de la información contable procesada, para que cumpla con los requisitos establecidos y sea de forma oportuna.

Objetivo: prevenir el uso inadecuado de los reportes emitidos por el sistema informático contable.

Alcance: Evitar la salida de información que muestre en forma clara y precisa los requerimientos necesarios para una adecuada toma de decisiones y revele la situación real de la entidad.

Normas a seguir:

1. La salida de información por medio de reportes deberá ser emitida por el usuario encargado.
2. Los reportes deberán mostrar la fecha, hora y ID del usuario que lo emitió.
3. Si los reportes no cumplen con las expectativas deberán ser modificados.
4. Los reportes deberán mostrar la información en forma clara, precisa y concreta, siendo la misma comprensible para los usuarios internos y externos.
5. Los reportes no serán emitidos por usuarios desautorizados.
6. Los reportes deberán detallar la información solicitada.
7. Se deberá verificar la integridad de la información emitida en reportes.
8. El sistema debe llevar un registro de cada uno de los reportes emitidos durante el periodo, permitiendo saber fecha, hora, nombre del reporte y la ID que la solicito.

Responsables del desarrollo, implantación y gestión:

1. El usuario que emita los reportes debe de verificar la integridad de los datos mostrados por el sistema, de preferencia será emitida por el supervisor de cada área.
2. Si el reporte no demuestra la estructura deseada deberá de informarse al usuario maestro que realice los cambios requeridos.
3. La veracidad de la información emitida por el reporte deberá de ser confrontada por el supervisor y usuarios encargados.
4. Solo el usuario maestro podrá realizar la verificación de reportes emitidos, en ningún caso dicha información deberá de ser eliminada del sistema.

2.3.5 Respaldo de la Información.
(ISO 17799 Num. 10.5.1; COBIT 4.0 dominios DS11.4/DS11.5)

POLITICA 1. Periódicamente se harán respaldos de la información existente en el sistema contable computarizado.

Objetivo: prevenir la pérdida de información dentro del sistema contable computarizado.

Alcance: realizar copias de reserva de la información existente en el software y en el sistema informático.

Normas a seguir:

1. El respaldo de la información se realizará para asegurar que toda la información esencial se puede recuperar después de un desastre natural, caso fortuito o falla del sistema operativo.
2. Se deberá realizar un respaldo periódico del sistema operativo y del sistema informático.

3. Deberá de etiquetarse dicho respaldo con la fecha en que se realizo y el periodo que esta abarcando.
4. Las copias de los respaldo deberán ser enumeradas y entregadas a los usuarios responsables del resguardo de los back-up.
5. Las copias deberán ser resguardadas en un lugar seguro, disminuyendo en caso de desastre el riesgo de perdida de información.
6. Los medios de reserva pueden ser dvd, cds, y deberán ser probados periódicamente para verificar su funcionalidad.

Responsables del desarrollo, implantación y gestión:

1. Los respaldos deberán de ser realizados por medio del usuario maestro.
2. El usuario maestro deberá de emitir una segunda copia que será entregada a la administración para resguardarse de cualquier peligro.
3. Se recomienda que a finales de cada mes se realice un respaldo mensual de la información o de acuerdo a las necesidades de la entidad.

3. Seguridad en Redes

3.1 Gerencia de la seguridad de la red

3.1.1 Autentificación del usuario para conexiones externas (ISO 17779 Num. 11.4.2; COBIT 4.0 dominio DS5.3)

Política 1: Las operaciones en línea se realizan ingresando un nombre de usuario registrado

Objetivo: Garantizar que las operaciones realizadas en línea con otra sucursal de la entidad, sean realizadas por la persona que corresponde y de acuerdo a los privilegios que se le asignen.

Alcance: Que cada uno de las operaciones realizadas en línea sea realizada en forma integra y se determine la autenticidad del usuario que realiza cada acción.

Normas a seguir.

1. Asignación de nombre de usuario en operaciones en línea con otras sucursales o con establecimientos externos.
2. Los Privilegios de la cuenta de usuario se restringirán únicamente para retroalimentar los datos, se deniega el acceso a borrar y/o modificar la información del sistema.
3. Las claves de acceso son únicas e intransferibles para cada usuario.

Responsables del desarrollo, implantación y gestión: Los responsables de autorizar las operaciones en línea es a cargo de la gerencia administrativa, el desarrollo e implantación se ejecutara por medio del departamento de contabilidad.

3.1.2 Identificación del equipo en redes

(ISO 17779 Numeral 11.4.3; COBIT 4.0 dominio DS5.4; DS5.7).

Política 1: Cada Usuario que haga uso de la red debe tener una Cuenta registrada.

Objetivo: Que a cada usuario se le asigne una cuenta de usuario con la que pueda ser responsable e identificable del uso de los recursos de la red, así como salvaguardar las actividades que ejecuta de las de otros usuarios de la red.

Alcance: Que cada usuario determine una cuenta de usuario con password, con la cual pueda acceder a la red. Y hacer uso de los recursos permitidos por su respectiva cuenta.

Normas a seguir:

1. Todas las claves de usuario serán diferentes e intransferibles, creadas por el usuario.
2. Toda clave de Usuario estará sujeta a privilegios y restricciones en la red.

Responsables del desarrollo, implantación y gestión: Los responsables de autorizar las cuentas de usuario será la gerencia administrativa, el desarrollo e implantación será ejecutado por el departamento o encargado de informática.

Política 2: No se utilizaran teclas de función que almacenen información de login o password

Objetivo: Evitar que personas no autorizadas hagan uso de las claves de otros usuarios

Alcance: Se restringirá el uso de teclas de función programables que permitan almacenar las claves de los usuarios en los equipos de cómputo o terminales de la entidad.

Normas a seguir:

1. Las aplicaciones de los programas usados por la entidad, en lo que se refiere a claves de usuario se eliminara el uso de teclas de función que almacenen las claves de los usuarios.

Responsables del desarrollo, implantación y gestión: El departamento o encargado de informático será el encargado de velar por la seguridad en los programas y accesos, eliminado los privilegios de uso de teclas de función que violenten la seguridad del usuario ante terceros de sus claves de acceso

3.1.3 Segregación en redes

(ISO 17779 Num. 11.4.5; COBIT 4.0 domínio DS5.3; DS5.4)

Política 1: No crear cuentas de usuario por defecto o de invitado

Objetivo: Garantizar que el uso y manipulación de recursos en la red sean atribuibles a un usuario en específico, es decir evitar la creación de cuentas para empleados temporales.

Alcance: Se deberá crear para cada usuario en la entidad una contraseña de uso en la red, con la finalidad de determinar responsabilidades ante el mal uso que se hagan de los recursos de la misma.

Normas a seguir:

1. La entidad creará una cuenta de usuario tanto para los empleados de planta, como los de tipo eventual a fin que cada uno sea responsable por el uso de los recursos de la red.

Responsables del desarrollo, implantación y gestión: El departamento de informática o responsable será el encargado de asignar las cuentas de usuario con previa autorización de la gerencia administrativa.

Política 2: Los privilegios de usuarios en la red deben ser únicamente para el desempeño de sus funciones.

Objetivo: Que cada usuario que haga uso de los recursos en la red posea únicamente los privilegios de seguridad necesarios para el desempeño de sus funciones.

Alcance: Se debe restringir que solo determinados usuarios puedan revisar, eliminar o modificar información de los programas y recursos de la red.

Normas a seguir

1. Cada cuenta de Usuario tendrá únicamente los privilegios necesarios para el desempeño de sus actividades.
2. Cualquier uso especial de la red será con previa autorización del encargado del área de contabilidad, el cual considerará si habilita o no, dicha acción dejando constancia escrita de dicho hecho.
3. Es prohibido transferir a otro usuario la clave de usuario para brindarle privilegios del uso de la red.

Responsables del desarrollo, implantación y gestión: El departamento de informática o encargado por defecto deberá velar por el uso y acceso que hacen los usuarios de la red, delimitando los privilegios que gozaran los mismos y que sean acorde a las necesidades para el desempeño de su trabajo

3.1.4 Control de la conexión de red
(ISO 17779 Num. 11.4.6 COBIT 4.0 dominio DS5.9, DS5.10)

Política 1: Deshabilitar o guardar físicamente las bocas de conexión sin uso.

Objetivo: Evitar el uso desautorizado de usuarios a conexiones de la red fuera de uso

Alcance: Que todas las bocas de conexión o puertos con acceso a la red de la entidad, que se encuentren en desuso puedan ser deshabilitados en los usos y privilegios de la red, o bloquear físicamente el acceso a ellos por parte de otros usuarios.

Normas a seguir

1. Cuando un equipo de la entidad, puerto o boca de conexión de un usuario quede en desuso, se deshabilitará para evitar que otro usuario ingrese a la red como otro usuario diferente.

Responsables del desarrollo, implantación y gestión: El departamento informático será el encargado de notificar a la gerencia administrativa de los puertos o conexiones sin uso, para que con la autorización de esta última se tomen las acciones correctivas necesarias.

Política 2: Delimitar el Acceso a Internet exclusivamente para Actividades de Trabajo

Objetivo: Que el acceso a Internet provisto para los Usuarios se encuentre delimitado exclusivamente para el

desarrollo de las actividades relacionadas al trabajo que desempeña

Alcance: Que el equipo computacional de los usuarios se encuentre delimitado únicamente para las necesidades operativas del mismo, y se lleve un control escrito de los accesos y privilegios con que cuenta cada Terminal.

Normas a seguir

1. Registrar los accesos y privilegios de los equipos de cada usuario
2. Cada usuario será responsable de un único equipo, ello con la finalidad de considerar responsabilidades ante desperfectos en los mismos o manipulaciones en la red originadas por un equipo de la entidad.
3. Cada usuario que no tenga restricciones para el uso de Internet deberá llenar una solicitud escrita, la cual deberá estar firmada por el mismo y el encargado del departamento delegado por la entidad, en la cual se compromete a ser sujetos de monitoreo de las actividades que realiza en Internet y a las siguientes prohibiciones:
   a. Acceso a páginas no autorizadas.
   b. Transmisión de archivos, reservados o confidenciales no autorizados.
   c. Descarga de software sin la autorización
   d. La utilización de Internet es para el desempeño de su Función y no para propósitos personales.

Responsables del desarrollo, implantación y gestión: La gerencia administrativa será la encargada de autorizar quienes de los usuarios tendrán acceso a Internet, definiendo las condiciones de su uso con el usuario, el

encargado de implementarlo será el departamento de informática o el responsable de dicha área, por medio de una solicitud escrita del usuario y aprobado con la firma de la gerencia.

3.1.5 Limitación del tiempo de conexión
(ISO 17779 Num. 11.5.6; COBIT 4.0 dominio DS5.5).

Política 1: El horario de uso en la red será únicamente durante la jornada laboral.

Objetivo: Que cada usuario haga uso de la red en horarios de trabajo determinados, asimismo el cierre de sesiones por inactividad en la misma.

Alcance: restringir que las sesiones dentro de la red de los usuarios se encuentren ociosas, o puedan ser uso de abusos de terceros, además determinar las horas efectivas de trabajo de los usuarios en la misma y que se encuentre dentro de los rangos de horarios de trabajo

Normas a seguir

1. Cerrar automáticamente la sesión del usuario después de 10 minutos de inactividad (el rango de inactividad puede varias de acuerdo a las necesidades de la entidad) a menos que puedan ser aseguradas por un apropiado mecanismo de fijación, ejemplo: una contraseña que protege el ahorrador de la pantalla.
2. El uso de la red es únicamente en horas de trabajo, y evitar el abuso en horas fuera de la jornada laboral.

3. Restricción del uso y horarios de acceso a Internet en las computadoras, además de la visita de páginas no confiables en la misma o material inadecuado.

Responsables del desarrollo, implantación y gestión: El responsable de llevar a cabo la delimitación de los Horarios de Uso del Sistema será el departamento informático, así como los cierres de sesión en tiempo de inactividad del usuario.

3.1.6 Seguridad en intercambio de información en red
(ISO 17779 Numeral 11.2.3; COBIT 4.0 dominio DS5.11 DS5.11, DS5.9)

Política 1: Restringir de la información confidencial procesada en terminales o computadores, y evitar la extracción de la misma por usuarios externos.

Objetivo: Que la información confidencial manipulada por determinados usuarios, sea restringido el acceso a copias en la red y los accesos a las impresores, fotocopiadores y envíos a medios extraíbles por personal desautorizado en la misma

Alcance: Que la información sensible de la entidad procesada en determinadas terminales se restringa la copia por terceros de la misma y el acceso de la misma en la red.

Normas a seguir

1. Las terminales con información sensible de la entidad tendrán códigos de acceso o claves para el envío de la misma a las impresoras y fotocopiadoras de la misma.
2. Las computadoras o terminales no tendrán acceso a dispositivos en medios magnéticos, CD regrabables, u otro

medio de transmisión de la información o los mismos contaran con clave.

3. El acceso a internet y/o correo electrónico en las computadoras y terminales con información sensible de la entidad será bloqueado.

Responsables del desarrollo, implantación y gestión: El encargado del departamento de informática será el encargado con previa autorización de la gerencia administrativa de restringir el intercambio de información desautorizado de las terminales de usuarios con información sensible de la entidad, deshabilitando puertos USB, accesos a Internet o correo electrónico por medio de password, y restricción hacia impresores y fotocopiadores.

Política 2: Restringir los accesos e intercambios de información por medio de Internet.

Objetivo: Prevenir el acceso desautorizado a los servicios en Internet.

Alcance: Que cada computador de la entidad delimite el acceso a Internet conforme a las necesidades laborales del usuario.

Normas a seguir

1. Cada usuario tiene acceso a la red únicamente con su login y/o password de usuario.
2. Control del acceso de usuario a los servicios de red a nivel local o externo.

Responsables del desarrollo, implantación y gestión: El encargado del departamento de informática con previa autorización de la gerencia será el encargado de delimitar los accesos a Internet correo electrónico tanto al interior de la entidad como el de uso externo.

Política 3: Los equipos de la entidad contarán con cortafuegos, anti spam, antispyware.

Objetivo: Que cada uno de las computadoras de la entidad posea programas actualizados para prevenir los ataques de virus informáticos, infiltraciones a la red local y a la información procesada al interior de la misma.

Alcance: Cada computadora de la empresa y sus sucursales, anexos y otras locaciones, posean programas especializados para salvaguardar la integridad y autenticidad de la información.

Normas a seguir

1. Cada computador tendrá programas para el resguardo de la información.
2. Cada computador se actualizará diaria o periódicamente los programas antivirus, firewall, antispyware y antispam.
3. Cada computador tendrá las licencias genuinas de los programas de resguardo que posea.

Responsables del desarrollo, implantación y gestión: La gerencia administrativa será la encargada de la aceptación y contratación de los paquetes utilitarios de antivirus, spyware, firewall, etc. El departamento de Informática o

encargado del área es el responsable de verificar que se encuentren actualizados en los equipos de la entidad, así como la vigencia de las licencias de los mismos.

Política 4: No violar la seguridad de las redes de la entidad.

Objetivo: Que el personal inexperto de la empresa violente las medidas de seguridad de la red con la finalidad de manipular permisos, restricciones a la información o cualquier acción que represente un ataque a la seguridad informática.

Alcance: Por medio de verificación y monitoreo de las computadoras de los usuarios, realizando pruebas sorpresivas en las cuales se verifique si los permisos originales del equipo han sido alterados.

Normas a seguir:

1. Realizar monitoreos durante la jornada laboral y verificar si los usuarios acceden a privilegios en la red denegados para su computador.
2. Los cambios significativos en los entornos del escritorio de los usuarios como accesos a programas ajenos a las operaciones que violenten la seguridad del equipo y de la red se deberán notificar a la administración.

Responsables del desarrollo, implantación y gestión: El encargado del departamento de informática o del área deberá monitorear que los usuarios no violen los permisos asignados a su usuario y/o privilegios en la red, Además la gerencia administrativa deberá sancionar estas faltas.

III. IMPLEMENTACIÓN

La implementación de medidas de seguridad, es un proceso Técnico-Administrativo. El cual abarcar toda la organización, sin exclusión alguna, el cual debe ser apoyado por la gerencia, ya que sin su apoyo, las medidas que se tomen no tendrán el respaldo necesario.

Se deberá tener en cuenta que la implementación de Políticas de Seguridad, conlleva problemas que afectan el funcionamiento de la organización. La implementación de un sistema de seguridad implica un incremento en la complejidad de la operatividad de la organización, tanto técnica como administrativamente.

Será necesario estimar cuidadosamente el costo – beneficio administrativo generado en la implementación, es fundamental notificar a todos los involucrados en las nuevas disposiciones y darlas a conocer al resto de la organización.

Se debe realizar una evaluación del factor humano, su entorno, controles con los cuales ejecuta su trabajo y evaluar los riesgos de área con la finalidad de determinar su vulnerabilidad y posibles consecuencias.

Luego de evaluar estos elementos se establece un criterio del nivel de seguridad que posee la entidad lo cual proporciona una base de análisis para establecer un programa de seguridad, el plan de acción y las normas y procedimientos a llevar a cabo.

Con el objeto de verificar que lo implementado proporciona un nivel aceptable de seguridad, se debe realizar una simulación

de eventos y acontecimientos que atenten contra la seguridad del sistema. Esto último deberá ser registrado, para retroalimentar y revisar que las políticas generadas en primera instancia son adecuadas.

IV. CONTROL Y MONITOREO DE LA IMPLEMENTACION.

Se considera que el control y monitoreo son los "ojos y oídos" de la dirección, ya que con estos se miden que las políticas sigan el curso esperado y encaminarlas por el rumbo deseado.

El control se encuentra conformado por las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos, detectados y corregidos.

El Objetivo que tiene el Monitoreo es contrastar el resultado final obtenido contra el deseado a fin de incorporar las correcciones necesarias para alcanzarlo, o bien verificar la efectividad de lo obtenido.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

1. Los dueños y administradores de las medianas empresas del sector comercio del municipio de San Salvador no poseen políticas de seguridad informática por escrito; mostrando poco interés en la capacitación del recurso humano en el área de seguridad informática.

2. Las medianas empresas del sector comercio no han adoptado estándares internacionales que regulen la seguridad informática en el procesamiento electrónico de datos contables.

3. Los gremios de profesionales de contaduría pública, han brindado poca cobertura en capacitar a los profesionales de la contaduría pública en el área de seguridad informática en el procesamiento electrónico de datos contables.

4. Los contadores, de las medianas empresas del sector comercio no aplican políticas de seguridad informática para el procesamiento electrónico de datos contables por lo que la misma es objeto de ser manipulada indebidamente.

5. Hay falta de interés por parte de las instituciones gubernamentales en establecer mecanismos, para crear leyes especiales que normen los aspectos relativos seguridad informático.

4.2. Recomendaciones

1. Que los dueños y administradores de las medianas empresas del sector comercio del municipio de San Salvador adopten una cultura de seguridad informática, plasmando políticas relativas en documentos como manuales o guías de usuarios; y capaciten a los usuarios adecuadamente.

2. Que las medianas empresas del sector comercio adopten estándares internacionales en materia de seguridad informática, para el procesamiento electrónico de datos contables tales como: ISO 27000, COBIT e ITIL.

3. Que los gremios relacionados con la contaduría pública impartan seminarios y capacitaciones relacionados con la seguridad informática en el procesamiento electrónico de datos contables.

4. Que los contadores de las medianas empresas del sector comercio, apliquen políticas de seguridad informática para el procesamiento electrónico de datos contables para prevenir y disminuir la manipulación indebida de la información contable.

BIBLIOGRAFIA

Libros:

Asamblea Legislativa de El Salvador, Año 2007, Codigo Civil, Editorial Juridica Salvadoreña, San Salvador, El Salvador.

Asamblea Legislativa de El Salvador, Año 2006, Recopilación de Leyes Triburarias, Editorial Juridica Salvadoreña, San Salvador, El Salvador.

Jovel Jovel, Roberto Carlos, Año 2008, Primera Edicion, "Guia Basica para Elaborar Trabajos de Investigación", Imprenta Universitaria, UES, El Salvador.

Normas Internacionales de Información Financiera, Año 2003, "Marco Conceptual para la Preparación y Presentación de los Estados Financieros", IASBI.

IT Governance Institute, Año 2005, "COBIT 4.0", Estados Unidos.

Trabajos de Investigación:

Niño Zambrano, Miguel Angel; Siler Amador, Donado; Flechas, Andres; Año 2007, Primera Edición, Programa de Ingeniería de Sistemas, "Seguridad Computacional", Universidad CAUCA.

Zapata, Carlos Alberto, año 2000, Tercera Edicion, "Administración y Manejo de Archivos Electronicos", Universidad de Quindio, Colombia.

Colindres, Salvador, Entrevista, Año 2002, "Historia de la Informatica en El Salvador", San Salvador, El Salvador.

Rodríguez, Luis Angel; Año 1995, Venturas Ediciones, S.A. de C.V.; "Seguridad de la Información en Sistemas de Computo", Mexico D.F., Mexico

Sorto Chavez, Idania Zoraida; Año 2003, "La Internet como estrategia de Comunicación Institucional y su impacto en el sector privado de El Salvador", Universidad Tecnología de El Salvador.

Sanders, Donald H; Año 2002, "Informatica Presente y Futuro", Mexico.

Direcciones Electronicas:

www.oni.escuelas.edu.ar/2004/BUENOS AIRES/571/Inform%Eltica3.html (Año 2004)

www.ati.es/does/internet/histintl.html#origenes (Año 2000)

www.revistainerforum.com (Año 2001)

www.pcm.gob.pe/portal_onegi/publicaciones/cultura/Lib5048/cap02.htm (Año 2005)

www.gestiopolis.com/canales/financiera/articulos/no%208/infocontable.htm (Año 2007)

ANEXOS

INDICE DE ANEXOS

GLOSARIO DE TERMINOS

Antivirus Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido o disquete.

Ataque Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese activo y lograr afectarlo.

Archivo Una colección identificada de registros relacionados.

Autorización Es el proceso de asignar a los usuarios permisos para realizar actividades de acuerdo a su perfil o puesto.

Código Malicioso Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Un caballo de Troya es ejemplo de un código malicioso.

Computadora Es un conjunto de dispositivos electrónicos que forman una máquina electrónica capaz de procesar información siguiendo instrucciones almacenadas en programas.

Confidencialidad Se refiere a que la información no sea divulgada a personal no autorizado para su conocimiento.

Control de Acceso Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo tecnológico.

Cuentas de Usuario
Es un identificador, el cual es asignado a un usuario del sistema para el acceso y uso de la computadora, sistemas, aplicaciones, red, etc.

Discos flexibles (diskettes)
Medios de almacenamiento magnéticos de información de 1.44 Mb llamados comúnmente discos de 3 ½.

Discos Ópticos Los discos ópticos son medios de almacenamiento de información que presentan una capa interna protegida, donde se guardan los bits mediante el uso de un rayo láser, éste al ser reflejado, permite detectar variaciones microscópicas de propiedades "óptico-reflectivas" ocurridas como consecuencia de la grabación realizada en la escritura. Un sistema óptico con lentes encamina el haz luminoso, y lo enfoca como un punto en la capa del disco que almacena los datos.

Disponibilidad Se refiere a que la información esté disponible en el momento que se requiera.

Falta administrativa
Es la consecuencia que resulta del incumplimiento de la normatividad.

Freeware (Software Libre)
Programas que se pueden bajar desde Internet sin cargo.

FTP Protocolo de transferencia de archivos. Es un protocolo estándar de comunicación, que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.
Filtro de Paquetes: Programa que intercepta paquetes de datos, los lee y rechaza los que no estén en un formato predefinido.

Firewall: un sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los Firewalls pueden estar implementados en hardware o software, o una combinación de ambos. Los firewalls son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de internet a redes privadas conectadas a la misma, especialmente intranets. Todos los mensajes que dejan o entran a la red pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplan con determinado criterio de seguridad.

Firewall Router: Filtro de paquetes que filtra el tráfico en base a la dirección destino y fuente.

FTP (File Transfer Protocol): Protocolo parte de la arquitectura TCP/IP utilizado para la transferencia de archivos.

Gusano Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas

Hacker: Persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

Hardware Se refiere a las características técnicas y físicas de las computadoras

HTML Lenguaje de marcado de hipertexto, (Hiper-Text Markup Languaje) es el lenguaje con que se escriben los documentos en el World Wide Web. A la fecha existen tres versiones de HTML. HTML 1, se sientan las bases para la disposición del texto y las gráficas, HTML 2 donde se agregan formas y HTML 3 (llamado también extensiones Netscape) donde se añaden tablas, mapas, etc.

HTTP. Protocolo de Transferencia de Hipertextos (Hiper-Text Transfer Protocol). Es el protocolo usado por el Word Wide Web para transmitir páginas HTML.

Integridad Se refiere a la pérdida o deficiencia en la autorización, totalidad o exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional o accidental.

Internet o World Wide Web (www)
Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes en donde cualquier usuarios consulta información de otra computadora conectada a esta red e incluso sin tener permisos necesarios acceder a dichos activos.

Intranet. Una red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es solo para uso interno.

Intrusión Es la acción de introducirse o acceder sin autorización a un activo tecnológico.
IP address (Dirección IP) Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

Mecanismos de seguridad o de control
Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.

Medios Magnéticos(medios de almacenamiento)
Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (diskettes, CDs, Cintas, Cartuchos, etc.).

Mecanismos de seguridad o de control
Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.

Módem Es un aparato electrónico que se adapta una Terminal o computadora y se conecta a una red de comunicaciones (red telefónica). Los módems convierten los pulsos digitales de una computadora en frecuencias dentro de la gama de audio del sistema telefónico. Cuando actúa en calidad de receptor, un módem decodifica las frecuencias entrantes.

Navegador: Aplicado normalmente a programas usados para conectarse al servicio WWW.

Normatividad Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización

Password Contraseña. Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a un computadora personal, sistema, aplicación o red en particular. Típicamente está compuesto de 6-10 caracteres alfanuméricos.

PPP Protocolo Punto a Punto (Point to Point Protocol). Implementación de TCP/IP por líneas seriales (como en el caso del módem). Es mas reciente y complejo que SLIP.

Protocolo Descripción formal de formatos de mensaje y de reglas que dos computadores deben seguir para intercambiar dichos mensajes.

Proxy Una substitución de direcciones, usado para limitar la información de direcciones disponibles externamente.

Proxy Server: Un server que se situa entre la aplicación cliente, como por ejemplo un web browser, y un server real. Intercepta todos los requerimientos al server real para ver si las puede resolver él. Si no, envia el requerimiento al server real.

Respaldo Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.

Riesgo Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene y su probabilidad de ocurrencia.

Router (direccionador) Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza en base a información de nivel de red y tablas de direccionamiento. El router se necesita cuando las dos redes utilizan la misma capa de transporte y tienen diferentes capas de red.

Servidor Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.

Sitio Web El sitio Web es una lugar virtual en el ambiente de Internet, el cual proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a el.

Software Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.

Software Antivirus Aplicaciones que detectan, evitan y posiblemente eliminan todos los virus conocidos, de los archivos ubicados en el disco duro y en la memoria de las computadoras.

Trojan Horse (Caballo de troya) programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema
que lo procesa.

URL. Localizador Uniforme de recursos (Uniform Resorce Locator). Sistema de direccionamiento estandar para archivos y funciones de Internet, especialmente en el Word Wide Web. El url esta conformado por el servicio (p. e. http://) más el nombre de la computadora (p. e. www.sfp.gov.ar) más el directorio y el archivo referido.

User-ID (identificación de usuario)
Se denomina al nombre de usuario con el cual accedemos a una página o sistema en el que previamente nos hemos registrado. Este nombre puede estar compuesto de letras, números o signos.

Usuario Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal, o dispositivo (hardware).

Virus Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o diskettes de computadoras.

Vulnerabilidad Es una debilidad de seguridad o hueco de seguridad, el cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencionado o accidental.

UNIVERSIDAD DE EL SALVADOR.
FACULTAD DE CIENCIAS ECONOMICAS
ESCUELA DE CONTADURIA PÚBLICA.

OBJETIVO:
Obtener una noción del conocimiento que tienen las medianas empresas del sector comercio de San Salvador, sobre la seguridad informática y la aplicación de manuales de seguridad informática.

Dirigido a:
Los Contadores y Auxiliares contables de las medianas empresas del sector comercio del departamento de San Salvador.

INDICACIONES:
Marque con una "X" el cuadro que corresponda a la alternativa que usted estime conveniente. Favor elegir solo una de las alternativas.

La información proporcionada será utilizada únicamente para fines académicos, garantizando absoluta y estricta confidencialidad.

1. ¿Procesa Información contable en computadoras?
   Si☐ No☐

2. ¿En que tipo de programas procesa la mayoría de la información contable?
   Software Especializado, hecho a la medida ☐
   Software Especializado, Comerciales ☐
   Software Utilitario o manualmente en hojas electrónicas (Como Microsoft Office) ☐

3. ¿Conoce en que consiste el término Seguridad Informática?
   Si☐ No☐

   Mencione en pocas palabras su concepto de Seguridad Informática:
   _____
   _____

4. ¿Qué tipos de procesos o políticas implementa para resguardar la información procesada electrónicamente?, mencione las 5 que considere más importantes.
   a)_____
   b)_____
   c)_____
   d)_____
   e)_____

5. ¿Cuántas de esta y otras políticas o procedimientos están plasmados en un Manual?
   - Muchas ☐
   - Pocas ☐
   - Muy Pocas ☐
   - Ninguna ☐

6. ¿Las personas que procesan y tienen acceso la información contable, son exclusivamente del área contable?
   Si☐ No☐

7. ¿Con qué frecuencia ha observado perdidas de información contable?
   - Muy frecuente ☐
   - Frecuente ☐
   - Poco Frecuente ☐
   - Casi nunca ☐
   - Nunca ☐

8. ¿En caso de que haya una pérdida de información, a qué atribuye la mayoría de las pérdidas?
   - Desperfectos en Hardware ☐
   - Desperfectos en Software ☐
   - Errores Humanos ☐
   - Otros (Especifique) ☐ _____

9. ¿Con qué frecuencia ha tenido diferencias entre la información contable procesada electrónicamente y la información documental (física)?
   - Muy frecuente ☐
   - Frecuente ☐
   - Poco Frecuente ☐
   - Casi nunca ☐
   - Nunca ☐

10. ¿En Caso de que haya diferencias en la información, a qué atribuye la mayoría de las diferencias?
    - Desperfectos en Hardware ☐
    - Desperfectos en Software ☐
    - Errores Humanos ☐
    - Otros (Especifique) ☐ _____

11. ¿Se ha dado alguna vez la divulgación de la información contable digital a personal no autorizado?
    Si☐ No☐

12. ¿Qué tan importante cree que es tener un Manual de políticas de seguridad informática para el procesamiento electrónico de datos?
    - Es muy importante ☐
    - Es importante ☐
    - Es poco importante ☐
    - Es nada importante ☐

13. ¿Cree que el no poseer un Manual de seguridad informática contribuye grandemente a que se de una manipulación indebida de la información contable?
    - Es muy probable ☐
    - Es probable ☐
    - Es poco Probable ☐
    - Es nada probable ☐

14. ¿Le gustaría implementar un manual de políticas de seguridad informática?

    Si☐ No☐ N/A☐

    Por qué:

    _____
    _____

15. Mencione 5 políticas que usted considera que se debe incorporar en un Manual de seguridad informática.

    a)_____
    b)_____
    c)_____
    d)_____
    e)_____

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓNICAS

ESCUELA DE CONTADURIA PÚBLICA

Objetivo: determinar los procesos utilizados por los usuarios al momento del Procesamiento Electrónico de Datos contables.

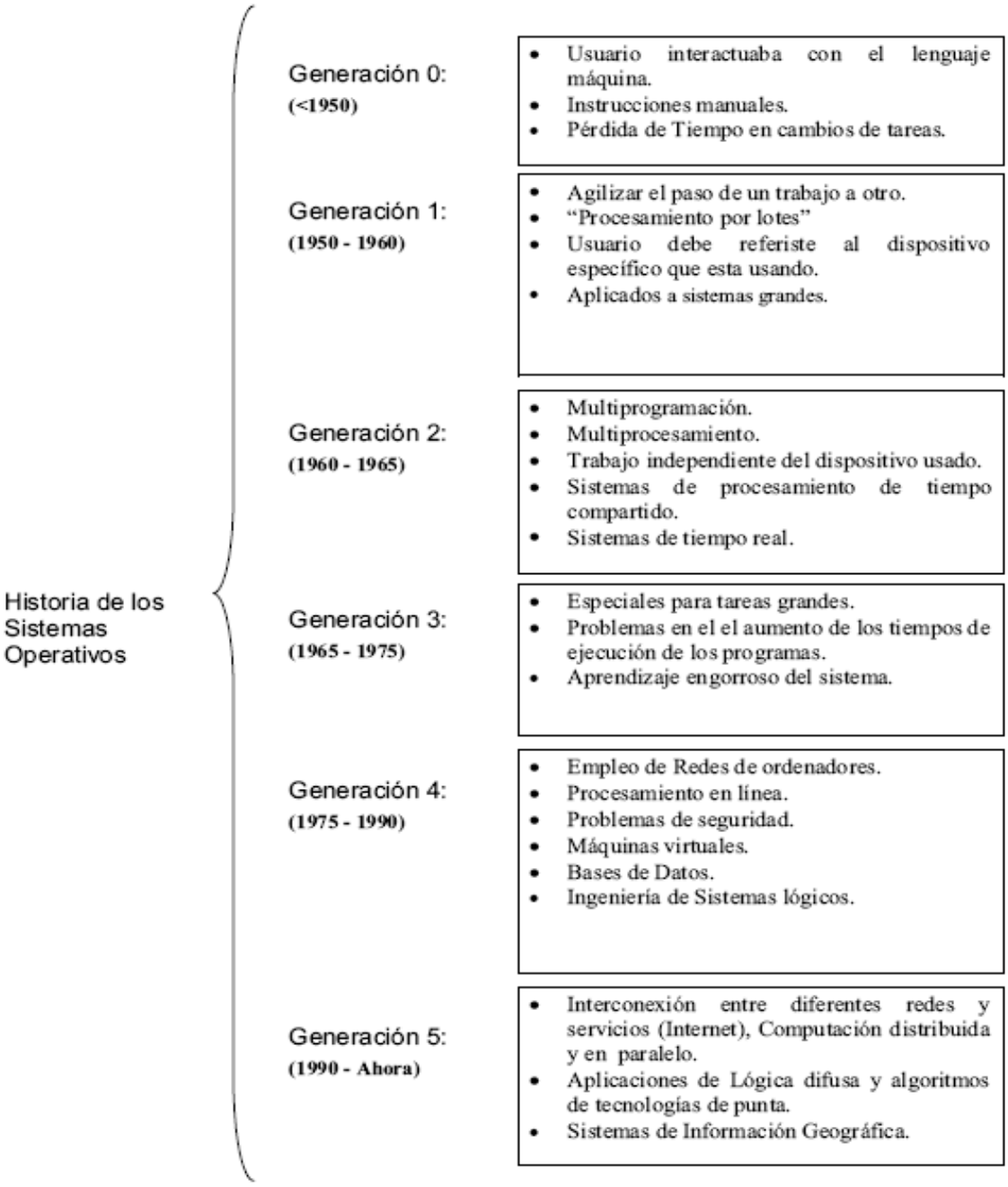
Cargo de la persona entrevistada:_____

1. ¿Qué procesos utiliza para acceder al programa donde procesa la información?
2. ¿De Dónde proviene y cómo le llega la información para el procesamiento?
3. ¿De qué forma introduce la información dentro del Sistema computacional?
4. ¿Qué técnicas o destrezas utiliza para verificar que la información introducida dentro del sistema es la correcta?
5. ¿A parte de usted, hay otras personas encargadas de introducir los mismos de tipos de datos contables en el sistema?
6. ¿En caso de que se de un error o un problema grave en proceso de introducción de datos, que procedimientos realiza?
7. ¿Qué tipos de reportes son los que más usa, y estos reportes llenas todas las expectativas de la información que requiere?
8. ¿Cómo culmina su proceso de procesamiento electrónico de datos contables?
9. ¿Cómo clasifica, guarda y archiva la información procesada?

PLAN ESCALONADO DE IMPLEMENTACION DE NIIF/ES

PLAN ESCALONADO PARA IMPLEMENTAR LAS NORMAS INTERNACIONALES DE CONTABILIDAD	DEBERÁN PRESENTAR SUS PRIMEROS ESTADOS FINANC. EN BASE A NICS POR EL EJERCICIO QUE INICIA EL
Consejo de Vigilancia Acuerdo del 31-10-2003, publicado en D.O. 06-01-2004 Empresas que emiten títulos valores que se negocian en el mercado de valores, así como los BANCOS y CONGLOMERADOS de empresas autorizados por la SSF. ***	01 de enero de 2004, otorgándoles el período de 12 meses para completar el proceso.
Intermediarios financieros no bancarios, sociedades de seguros, asociaciones y sociedades cooperativas que no emitan títulos valores que se negocian en el mercado de valores.	01 de enero de 2005, otorgándoles el período de 24 meses, a partir del 01 de enero de 2004.
El resto de empresas, excepto aquellas clasificadas por CONAMYPE como Medianas, Pequeñas y Micro Empresas.	01 de enero de 2005, otorgándoles el período de 24 meses, a partir del 01 de enero de 2004.
Las organizaciones no lucrativas (ONGs) que reciben fondos del exterior para cumplir con su finalidad y aquellas que realizan actividades de intermediación financiera.	01 de enero de 2005, otorgándoles el período de 24 meses, a partir del 01 de enero de 2004.
La mediana empresa *(toda unidad económica que tiene hasta 100 ocupados y que sus ventas anuales son hasta el equivalente de 3,.746 salarios mínimos mensuales urbanos, excluyendo aquellas que tienen ventas anuales menores al equivalente a 4,762 salarios mensuales mínimos con 50 o menos ocupados)* y la pequeña empresa *(toda unidad económica que tiene hasta 50 ocupados y que sus ventas anuales son hasta el equivalente de 4,762 salarios mínimos mensuales urbanos, excluyendo aquellas que tienen ventas anuales menores al equivalente de 476.2 salarios mensuales mínimos con 10 o menos ocupados.*	01 de enero de 2006, otorgándoles el período de 36 meses, a partir del 01 de enero de 2004.
Las microempresas *(toda unidad económica que tiene hasta 10 ocupados y ventas anuales hasta el equivalente de 476.2 salarios mensuales mínimos urbanos.*	No están afectas a esta regulación; pero podrán adoptar las NICs en forma voluntaria, cuando así lo estimen conveniente.

ESQUEMA DE HISTORIA DE LOS SISTEMAS OPERATIVOS



Fuente: tesis "Seguridad física: sus implicaciones e implicaciones" de Cristian F. Borghello 2001

FORMATO PARA EL REGISTRO DE USUARIOS Y PERMISOS EN LA RED

Recurso del sistema		Identificación del usuario	Tipo de acceso	Permisos otorgados
Número	Nombre			

Fuente: tesis "Seguridad física: sus implicaciones e implicaciones" de Cristian F. Borghello 2001

TEST DE SEGURIDAD COMPUTACIONAL PARA USUARIOS EN REDES

El siguiente es un test de seguridad que debe aplicar el administrador de la red a todos los usuarios de la misma, para medir los niveles de riesgo en materia de seguridad de la información de los usuarios. En algunos casos las respuestas suelen parecer obvias, pero al colocarles el grado de sinceridad a las respuestas ya dejan de ser tan obvias. Las respuestas correctas del test son de amplio conocimiento por los administradores de la red, así que si usted diligenció el test y tiene alguna duda con respecto a las respuestas, entonces diríjase al administrador de su red. El tomará los correctivos del caso a partir de sus respuestas.

Nombre del usuario :
Cargo en la entidad:
Número de la oficina:
Identificación del equipo:
Fecha:

1. Con respecto al manejo de contraseñas.

a. Comparto mi contraseña de acceso al servidor con mis compañeros de trabajo.
SI ☐ NO ☐

b. Mi contraseña tiene menos de 8 caracteres.
SI ☐ NO ☐

c. Mi contraseña tiene por lo menos un carácter especial, es decir (!"#$%&/()=?¡) entre otros.
SI ☐ NO ☐

d. Mi contraseña tiene que ver con algo de mi lugar de trabajo, familia o amigo.
SI ☐ NO ☐

e. Mi contraseña tiene que ver con una secuencia de sólo números, placa de mi transporte o la identificación de algún documento.
SI ☐ NO ☐

f. Acostumbro a repetir mis contraseñas para no olvidarlas.
SI ☐ NO ☐

g. Para que no se me olvide la anoto en un sitio seguro, pero cercano a mi lugar de trabajo.
SI ☐ NO ☐

h. Acostumbro utilizar programas que generen mi contraseña por mi.
SI ☐ NO ☐

i. Mi contraseña ha sido descifrada alguna vez.

2. **Con respecto al manejo de la información.**

   a. Mantengo una copia actualizada en el servidor.

   SI ☐ NO ☐

   b. La información crítica de la empresa la manejo encriptada.

   SI ☐ NO ☐

   c. Me llevo trabajo de la empresa para adelantarlo en mi casa.

   SI ☐ NO ☐

   d. Instalo programas que descargo de internet, sin autorización del administrador de la red, que me facilitan un poco mi trabajo.

   SI ☐ NO ☐

   e. Envío información crítica por correo electrónico sin encriptarla.

   SI ☐ NO ☐

   f. Sé manejar completamente el antivirus que se me instaló en mi equipo.

   SI NO

   g. Actualizo regularment(vez al mes) mi an s.

   SI ☐ NO ☐

   h. Ejecuto mi antivirus por lo menos una vez al día.

   SI ☐ NO ☐

   i. Cualquier archivo que llegue a mi equipo, sea desde una página web, correo electrónico, servidor de archivos o diskette es vacunado.

   SI ☐ NO ☐

   j. He perdido información por causa de algún virus.

   SI ☐ NO ☐

3. **Con respecto al equipo.**

   a. Mantengo el equipo en un lugar fresco, recomendable e ideal.

   SI ☐ NO ☐

   b. Se le realiza el mantenimiento de software necesario por personal especializado.

   SI ☐ NO ☐

c. Se le realiza el mantenimiento de hardware necesario por personal especializado.
SI ☐ NO ☐

d. Es portátil.
SI ☐ NO ☐

e. En el caso que no sea portátil, permanece en el mismo sitio constantemente.
SI ☐ NO ☐

f. Permanece completamente cerrado.
SI ☐ NO ☐

g. Evito ingerir alimentos cerca del equipo.
SI ☐ NO ☐

h. Instala hardware por su propia cuenta y no avisa al personal encargado.
SI NO

i. Establece configuraci☐ y las cambia cuan☐esea sin informar al personal encargado.
SI ☐ NO ☐

j. Instalo programas sin diligenciar debidamente la licencia de software ante el personal encargado.
SI ☐ NO ☐

k. Poseo alguna UPS que respalde la ausencia de energía.
SI ☐ NO ☐

l. He perdido información importante por causa de la interrupción de energía eléctrica.
SI ☐ NO ☐

m. Se ha dañado algún elemento de mi equipo por causa de la interrupción de la energía eléctrica.
SI ☐ NO ☐

4. Comentarios

_____

_____

_____

Fuente: tesis "Seguridad física: sus implicaciones e implicaciones" de Cristian F. Borghello 2001

ANEXO VIII

FORMATO DE MATRIZ PARA EVALUAR RIESGOS EN RECURSOS INFORMATICOS

Recurso del sistema		Riesgo (R_i)	Importancia (W_i)	Riesgo Evaluado ($R_i * W_i$)
Número	Nombre			

Aplicación de la matriz para evaluar riesgo en recursos informáticos.

Para implementar una política de seguridad informática aplicable a los recursos informáticos se debe realizar una evaluación de riesgos, con el cual se pretende calcular la posibilidad de que ocurra una amenaza.

Inicialmente se debe realizar una serie de preguntas asociadas al recurso informático entre las cuales se pueden mencionar:

1. ¿Qué riesgos son atribuibles o de interés al equipo?
2. ¿con qué frecuencia pueden ocurrir los mismos?
3. ¿Qué consecuencias traerá a la entidad esos riesgos?

Una vez obtenida la lista de riesgos atribuibles a los equipos se procede a realizar un cuadro de evaluación de riesgos(cuadro 1):

TIPO DE RIESGO	NIVEL DE RIESGO
• Robo de Hardware • Robo de información • Vandalismo • Terremotos	ALTO ALTO MEDIO BAJO

Para la cuantificación del riesgo de perder un recurso es posible asignar valores numéricos de 0 a 10 y determinar de una manera su importancia (siendo 10 el recurso más alto).

El riesgo del recurso será el producto de su importancia por el riesgo de perderlo.

$$WR_i = R_i * I_i$$

Luego con la siguiente formula es posible calcular el riesgo general de los recursos de un área en específico, por ejemplo al calcular el riesgo de una red se aplicaría la fórmula siguiente:

$$W_R = \frac{(WR_1 * I_1 + WR_2 * I_2 + ... + WR_n * I_n)}{I_1 + I_2 + ... + I_n}$$

Retomando el cuadro de evaluación de riesgos (cuadro 1), se tiene:

Recurso	Riesgo (R_i)	Importancia (I_i)	Riesgo Evaluado (R_i*I_i)
Router	6	7	42
Gateway	6	5	30
Servidor	10	10	100
PC's	9	2	18

En el cuadro anterior se puede apreciar que el recurso de mayor importancia es el servidor, para evaluar la vulnerabilidad del área se procede a aplicar la fórmula mencionada anteriormente:

$$W_R = \frac{42 + 30 + 100 + 18}{7 + 5 + 10 + 2} = 7{,}92$$

Se puede visualizar que el riesgo total de la red es de casi 8 puntos sobre la base de 10, debería evaluarse los elementos ligados con el servidor.

Fuente: tesis "Seguridad física: sus implicaciones e implicaciones" de Cristian F. Borghello 2001

CONFESIONES DE UN HACKER

Carlos usurpa dinero de tarjetas de crédito desde su computadora, y sus víctimas las escoge al tin marín de do pingüé. El cursor puede detenerse en la cuenta de crédito de cualquier salvadoreño, y en las narices de las autoridades, que están maniatadas por la ausencia de una ley que regule de manera específica las actividades de los hackers. La banca prefiere callar ante la fragilidad de sus sistemas de seguridad, que permiten que alguien como Carlos entre como si fuera su casa, tome lo que quiera y salga por la puerta silbando.

Fernando Romero Fotos de LA PRENSA/Tulio Galdámez

Fecha de actualización: 12/23/2007

Sus dedos delgados se mueven con rapidez mientras en sus ojos se reflejan, de abajo hacia arriba, nombres y números. Son cuatro series de cuatro números, similares a los grabados en altorrelieve en las tarjetas de crédito. También pasan números de claves personales, números de saldos actuales y números de límites de crédito. Números útiles, que le sirven para comprar artículos por internet. "Si se dan cuenta mis tatas de lo que hago, me van a fregar." Ese pensamiento no lo deja tranquilo, pero no lo amilana. Mantiene clavada su mirada en el monitor y presiona cada tecla con precisión, atento de que en nadie de su familia se despierte la curiosidad por lo que hace. Pasan los minutos y se pone más nervioso, consciente de su travesura. Con cada compra aprobada, abre más sus ojos, sonríe, se ajusta su gorra y tose levemente. Está satisfecho.

Hackeado. Este es el "link" del Ministerio de Trabajo, en Google, el 22 de octubre de 2007. Se lee "Hacked by Turok". El ministerio informó que en ese mes su sitio web fue bloqueado al menos dos veces por ese hacker.

En su pantalla hay tres ventanas activas. La primera, de internet, para navegar y acceder a los sitios de ventas en la red. La segunda, donde se le facilita el uso de un servidor proxy, que es un intermediario con el que transita en la web para no exponer su propio Internet Protocol (IP) o identificación. Es una especie de disfraz que lo hace parecer un usuario diferente que se encuentra en otro país del mundo. Y la tercera ventana, la más valiosa, que contiene una base de datos con toda la información crediticia y personal de la mayoría de la población salvadoreña.

Con esa herramienta, que le sirve para alterar la identidad y la ubicación de su computadora, y con la información del banco de datos, puede comprar lo que quiera.

No lo dudó aquella tarde junto a sus amigos en su casa. Compró más de 10 laptops por internet. Gastó en total $17,000, todo con dinero ajeno. Carlos estaba sobrado de razón al justificar su miedo. Si se daban cuenta sus tatas, lo iban a fregar. Si se daba cuenta la Policía, lo iban a detener.

Entre sus amigos que lo acompañaban, uno de ellos le propuso ser destinatario de las computadoras portátiles a cambio de recibir su parte de la ganancia cuando las vendieran, a mitad del precio original. A él le pareció buena idea, porque no quería que sus padres lo descubrieran por ningún motivo, y además sabía que de esa manera, ofreciéndolas como gangas, las laptops se iban a vender mucho más rápido.

"El dinero de esa gente me vale, de todos modos no es mi pisto", se justificaba a sí mismo, con la certeza de que como fuera que vendiera las computadoras iba a tener buenos ingresos. Esa tarde, sin una autoridad que lo reprendiera ni moral que lo hiciera retroceder, el hacker violó a placer la seguridad informática del sistema financiero salvadoreño. De los usuarios, sin saberlo ellos, usó el dinero de sus créditos como le vino en gana.

Pasaron días antes de que vendiera todas las laptops. "Esa fue la vez que más dinero gasté", recuerda hoy, casi un

año después. Corre octubre, es sábado, y Carlos ha abierto las puertas de su casa para una plática. Sobre las paredes amarillas no cuelgan diplomas ni títulos ni fotos familiares. Hay filas de libros en el suelo y calor.

Sus padres están en casa con una pareja de amigos. Él se encuentra sentado, bebiendo una cerveza en su día de descanso —de su lugar de trabajo solo dice que es una empresa relacionada con la informática—. Usa una gorra azul, su preferida, cuya visera esconde a medias sus cejas pobladas; tiene una tos leve y lo acusa una mirada nerviosa que trata de delatar sus secretos, pero su boca ya se le adelantó.

Tiene 25 años y es el menor de dos hermanos. Calcula que ya tiene más de una década de haberse iniciado en la computación, y cuenta que su primera diablura como hacker consistió en introducirse en las listas electrónicas de su colegio, a manera de juego, donde podía alterar las calificaciones. Incluso un día les elevó varias notas a una compañera que le gustaba y a sus amigos. Nadie lo descubrió, pero desde entonces supo que lo que hacía no estaba bien.

Mientras pasaba el tiempo, y el colegio, y llegaba la universidad, se perfeccionó en el uso de GNU/Linux, de Unix, un sistema operativo equivalente al Mac OS, de Apple, o al Windows, de Microsoft, al que le dedicó muchas horas de aprendizaje, hasta que afinó su manejo y empezó a jugar con lo que sabía. Descubrió que Linux no tiene registro de los usuarios, y esa característica que sirve de camuflaje es la que lo vuelve atractivo para los hackers, como corroboran distintos expertos en informática. Con este sistema operativo, aprendió a diseñar programas, a evolucionar los existentes e incluso a crear virus.

Sobre Linux, explica que se puede conseguir en internet y que su descarga es gratuita, pues la licencia es de libre acceso. Además, es compatible con computadoras de todas las marcas, y los usuarios pueden modificar las distribuciones y los programas a su antojo y compartirlos.

Las distribuciones son como las versiones de Windows —95, 98, XP, Vista— y Apple —Mac OS y sus números—, con la diferencia de que en Linux los usuarios configuran el sistema operativo.

Carlos completó su banco de datos cuando extrajo información del Registro Nacional de las Personas Naturales (RNPN).
El Gobierno carece también de estricta seguridad en sus redes informáticas.

Y tiene más características que son especificadas por Raúl Funes, experto en seguridad informática de Next Genesis, S. A., quien menciona la facilidad que da el sistema para crear herramientas de hackeo, además del acceso a los proxy, que ocultan a los hackers cuando rompen sistemas de seguridad y se infiltran en redes informáticas para robar bases de datos, introducir virus o, lo más infantil según Carlos, bloquear páginas web.

Funes tiene más de 10 años dentro del área de seguridad informática —el mismo tiempo que cuenta Carlos como hacker— y también opera con Linux. En su oficina, escudado por dos computadoras y un monitor de vigilancia,

piensa con detenimiento antes de responder si es posible que un hacker logre penetrar la red de seguridad de un banco, y robe su base de datos con los números de cuentas y los datos personales de todos sus usuarios. "Es factible —se le escucha tras varios segundos—, todo depende del grado de bien o mal configurados que estén los sitios." Pero subraya que no solo de esa manera es posible obtener una base de datos, pues ahora cualquier empleado tiene acceso a la información de la institución en que trabaja, y nadie tiene a cargo un control minucioso sobre correos electrónicos o memorias USB dentro de las empresas, o incluso sobre las mismas carteras de clientes de los vendedores —en el caso de las tarjetas de crédito—, quienes se quedan con ellas aun después de abandonar los bancos.

Carlos titubea al aclarar cómo obtuvo la base de datos de la institución emisora de tarjetas de crédito, si acaso fue mediante un amigo que trabajaba en esa empresa o si él mismo laboró ahí. Apenas asoma una sonrisa jactanciosa y vuelve a toser. Calla. Y solo después de un breve silencio hace su confesión, en tono serio y con voz muy baja, para evitar que lo escuchen sus padres: "Esa información me la robé luego de vulnerar el sistema informático del banco". Y vuelve a cerrar sus labios. Sobre este asunto no mencionará una palabra más.

Se excusa por un momento, y se levanta de su asiento para ir a despedir a sus padres, que le avisan que saldrán con sus amigos y que regresarán pronto; y ya de pie, antes de irse, apenas se le alcanza a percibir entre murmullos: "Ahora sí vamos a poder hablar mejor". Ya ha pasado más de media hora desde que comenzó la conversación. La cerveza está a la mitad. Carlos regresa pasado un minuto, toma la botella y sorbe un poco, y hace la invitación a acercarse a su monitor. Ya sentado frente a su computadora, se acomoda para proseguir con su historia.

Dice que nunca le ha gustado usar créditos que tienen límites bajos y, en su particular escala de valores, se presenta como alguien ético por el hecho de no desvalijar a quienes tienen menos ahorros en sus cuentas. "Les quito solo a los que tienen de $5,000 para arriba", justifica su concupiscencia enseguida, mientras da el último trago a lo que le queda de cerveza.

Entre los que superan esa cantidad, tampoco es selectivo, pues los escoge al azar, según el devenir de sus caprichos, que no tienen restricción. Compra lo que se le place a la hora que sea, pero explica que se abstiene de comprar bienes suntuosos, como vehículos, por su temor a ser descubierto; por eso, dice, siempre procura mantener un perfil bajo, para pasar desapercibido. Aunque admite que ya ha pecado, como la noche cuando gastó $3,000 en apuestas en un casino en línea con el número de tarjeta de crédito de otra persona, o como cuando madrugó dentro de un sitio de pornografía en directo en el que la permanencia costaba $5 el minuto, y siempre con crédito ajeno.

Recolección. A Carlos le llevó casi dos años compilar su banco de datos. Para ello tuvo que burlar la seguridad de instituciones privadas y de Gobierno. También intercambió información con otros hackers de su comunidad.

Sus diversiones como hacker también incluyen bloquear correos electrónicos y sitios en la web, de cualquier naturaleza, e introducir virus en redes, además de las innumerables ocasiones en las que, apoyado en su base de datos, ha efectuado recargas de minutos para hacer llamadas desde $50 y más, desde su teléfono móvil, en una empresa de telefonía celular. Una vez recargó su crédito para llamadas por $150 en un solo día, hasta que en la telefónica notaron lo extraño de las operaciones. Después se le volvió más enredado el trámite, le solicitaban todo tipo de identificación, aunque no era problema para él porque tenía todos los datos de la persona que escogía para usar su crédito, pero de a poco los engorrosos requerimientos lo desalentaron. Pasó el tiempo y con él se disminuyó la periodicidad de las recargas. Ahora las adquiere solo cuando lo necesita.

Siempre evita que se tengan registros de él más que los necesarios, como DUI y NIT, "pero jamás una tarjeta de crédito", dice con ironía, y asegura que es hasta hoy que tiene un trabajo que debió, por requerimiento, abrir una cuenta bancaria. Es persistente por permanecer en las sombras del anonimato, tratando de estar al margen de los registros, "¡para no aparecer yo también en las bases de datos y no me puedan joder otros hackers!", remata, y suelta una risa.

Cuenta que ha sido contratado por varia gente, sin nombre ni apellido, para encontrar datos personales, y hasta ha vendido los números de las tarjetas de crédito a otros hackers dentro su comunidad informática, por los que ha llegado a cobrar hasta $500 por 15 números. El grupo al que pertenece Carlos lo integran, además de otros hackers, los llamados cashiers, que son troqueladores o clonadores de tarjetas de crédito, que cometen desfalcos en cajeros automáticos en todo el mundo. Él les vende los datos y ellos, con máquinas reproductoras de tarjetas de crédito, elaboran los clones, van a los cajeros y vacían las cuentas.

Carlos habla ya con más soltura y describe su comunidad. Explica que los hackers se rigen bajo ciertas reglas, como no perjudicarse entre sí, o como que no pueden llamarse a sí mismos hackers, hasta que sus colegas les dan ese título, que varía según sus acciones.

Cuestión de sombreros

Y distingue así a los hackers de sombrero blanco (white hat), de conocimientos avanzados en informática, pero que no pretenden lucrarse. Son los mismos a los que Funes llama hackers éticos, que bloquean por moral, por salud mental o incluso por valores religiosos, páginas web de pornografía, o que desbloquean sitios hackeados y crean redes de seguridad informática para protegerse de los ataques de otros hackers. También los que trabajan dentro de empresas como Microsoft o Google, para su protección, y los desarrolladores de programas.

A Carlos no le llama la atención andar por ahí hackeando sitios web de pornografía u otros de carácter inmoral, aunque sí admite que hay algo que siempre le ha atraído del mundo blanco de los hackers, y es que él podría ganar mucho dinero, "legalmente", si fuera contratado en las áreas de seguridad informática de las empresas. Pero él camina en otra tierra, menos conocida por la gente y donde los hackers se visten con sombrero negro: el mundo de los black hat, conocidos también como crackers, que son los que bloquean las web, descifran contraseñas de los correos electrónicos o los dispositivos de seguridad en los sistemas informáticos, y atacan las redes institucionales o a los usuarios particulares con virus; además, extraen de cualquier sitio —particular, empresarial o gubernamental— información confidencial o datos para su comercio o para su uso personal, que deriva en la comisión de delitos como estafas y hasta actos de terrorismo. Los black hat pueden llegar a ejecutar todas esas acciones sin dejar el mínimo rastro, gracias a la perfección de sus técnicas de hackeo. El mayor reto de Carlos en su vida ha sido no dejarse descubrir. Hasta este momento ha tenido éxito.

Carlos hace deslizar por su monitor la base de datos, aunque en toda la conversación se ha resistido a decir a qué institución pertenece. La muestra orgulloso, sabe que el suyo no es un caso común de acceso a información, que no la encontró por ahí navegando a la deriva en la red. Incluso, el disco que contiene el banco de información lo tiene secretamente guardado, en un lugar que considera muy seguro, fuera de su casa, como una especie de coartada por si algún día lo descubren y llegan a tocar a su puerta. Acerca de ese momento, sabe que, lejano o no, es posible que se presente.

Y ya han estado cerca de dar con él, como cuando la emisora de tarjetas de crédito percibió que alguien había burlado su red de seguridad, y comenzó una investigación para descubrir el origen de la infiltración. Funes llama a esta operación "investigación forense", y consiste en revertir el proceso de hackeo, es decir, localizar el punto vulnerable por donde el hacker traspasó la barrera de seguridad y luego detallar el proceso que siguió para escabullirse sin ser detectado. Durante esos días, Carlos salía lo menos posible a la calle, incluso se le cruzó la idea de abandonar unos meses el país. Pasaba recluido en su casa, hasta donde le fuera posible sin levantar las sospechas de su familia, y se ahogaba en sus propios nervios mientras visualizaba en su mente a los policías esposándolo, a sus padres decepcionados y sus fotos en los medios.

No llaman su atención estudios de Ingeniería en Computación. Como hacker, se jacta de que sus conocimientos en informática son mucho más avanzados.

Dice que no teme tanto a un juicio como a que lo arresten. En ese instante, abandona las cuentas de crédito y despliega un archivo que muestra la Ley de Bancos y el Código Penal de El Salvador, y menciona algunos delitos de los que lo podrían acusar, como la estafa o el uso del nombre de otra persona. Lo hace para demostrar que está informado del alcance legal de sus actividades, y además consciente de que sus travesuras como hacker no son tan infantiles, porque lo convierten en un delincuente.

De lo que no está consciente Carlos es de que la Fiscalía General de la República (FGR) no tomaría cartas en el asunto si se le llegara a presentar una denuncia sobre un caso como el suyo, como lo sostiene un abogado fiscal que pide la omisión de su nombre, y que asegura que no hay una ley salvadoreña que encierre y sancione la actividad del hackeo o que incluya el término "hacker", por lo que la institución se vería incapaz, según él, por falta de instrumentos legales, de acusarlo. Esto se verificó mediante la Unidad de Receptoría de la Fiscalía, y se corroboró que nunca ha llegado una denuncia de este tipo al departamento, que es el encargado de recoger y distribuir los casos a todas las unidades fiscales.

La postura del ministerio público, para el abogado Henry Campos, no es más que una señal de ignorancia de las leyes que sufre la institución, pues si bien Campos reafirma la aclaración de la Fiscalía de que no existe una terminología del hacker ni su actividad está incluida en el Código Penal, los delitos que se cometen mediante el hackeo sí están sancionados por la ley salvadoreña, algo que hasta Carlos sabe muy bien. Esto también lleva al abogado a determinar la posibilidad de que lo que podría existir es una falta de voluntad o incapacidad de gestión para darles cobertura a estos casos, que incluso son sometidos a criterios de eliminación, según Campos, debido a la sobrecarga de trabajo fiscal: "La misma Fiscalía dijo que necesitaba presupuesto para contratar a personal, porque por cada fiscal había alrededor de 200 casos en espera de ser atendidos".

Pero igual, Carlos le sigue temiendo a la ley: "Si me agarran, ya detenido, ven qué se inventan para joderme". Además, conoce casos de hackers en Estados Unidos y Europa en los que estos son juzgados y condenados a pagar con cárcel sus acciones, pues dentro de esas leyes extranjeras sí se definen los delitos que son producto exclusivamente del hackeo. Y así lo confirma Manuel Chacón, representante de Business Software Alliance (BSA) en El Salvador, quien agrega que en estos países (Estados Unidos y los de la Unión Europea) se hace efectiva la jurisprudencia, es decir, que aunque no esté regulada una ley que castigue la actividad de los hackers, sí existe un conjunto de sentencias por delitos similares que les sirven como precedente a los tribunales para poder sancionar esas acciones. Chacón lamenta la falta de voluntad judicial en El Salvador para atender estos delitos informáticos, aunque acepta que como BSA nunca han tomado la iniciativa de denunciar este tipo de casos en el país, ya que le atribuye al Estado tanto la prevención como la ejecución de las medidas sancionadoras: "No podemos hacer nada porque es decisión soberana y responsabilidad del Gobierno de cada país la creación de leyes para que pueda haber denuncias y haya castigo para quienes hacen esto".

Para continuar jugando a que no lo pillen, Carlos siempre apuesta su invisibilidad a la seguridad que le ofrece el uso del servidor proxy de web, que lo hace parecer un usuario navegando en otro país. Han pasado tres horas y

una cerveza más. Los padres de Carlos se han retrasado un poco, aunque sí acaba de llegar un primo. La plática se ha extendido, y curiosamente se nota cierta satisfacción en su rostro; ahora ya no exuda tensión, parece estar liviano, luego de poner en el escaparate su doble vida. Mientras echa un vistazo a su reloj, brota una de las últimas preguntas, que no responde hasta luego de un momento, y con desdén contesta que no lo sabe y que, además, le interesa muy poco: ¿Y los afectados?

En El Salvador aún no prolifera el iPhone, pero ya hay telefónicas ofreciendo activarlo e insertarle sus chips, sin revisar si se encuentra hackeado.

La Fiscalía niega tener casos de estafas por hackers, y eso lleva a preguntarse dónde están las denuncias de los perjudicados. Y si hay uno o más Carlos en El Salvador que siguen comprando por internet con créditos de otras personas, por qué no hay nadie reclamando que en sus estados de cuenta aparecen gastos que jamás hizo. El hilo se enmaraña, y resulta difícil alinear el robo de la base de datos, las compras en la red, el cargo registrado por la emisora de tarjetas de crédito, el cobro correspondiente y la denuncia del tarjetahabiente; y es en ese último elemento donde se delinea el curvilíneo signo de interrogación, porque precisamente denuncias es lo que no hay.

Los archivos del Centro para la Defensa del Consumidor con denuncias del año anterior a la fecha no descubren nada —como lo señala Mauricio Boulogne, del área de comunicaciones—, no aparecen casos que describan cargos a cuentas por compras que nunca fueron hechas por los dueños de las tarjetas. Como si la gente pagara ciegamente lo que se les cobra en los estados de cuenta. Esta institución tiene denuncias de estafas que incluyen tarjetas de crédito, pero son casos de robo de las mismas, o por los secuestros express, o por el phishing, que es la elaboración de una réplica del sitio web del banco, donde se recogen los datos de los usuarios que visitan la página usurpadora, sus números de cuentas y contraseñas para estafarlos.

Cuando se aborda el tema del phishing, Carlos suelta una mueca burlona, y dibuja un gesto de descalificación. Los que hacen phishing no son hackers. "Son ladrones choleros", lanza su dictamen con desprecio, y es porque son fáciles de descubrir y porque además no tienen un conocimiento elevado de la informática, como él, dice en tono de broma. Se pavonea. Pero sigue sin saber responder quién paga por sus caprichos.

Los usuarios hablan

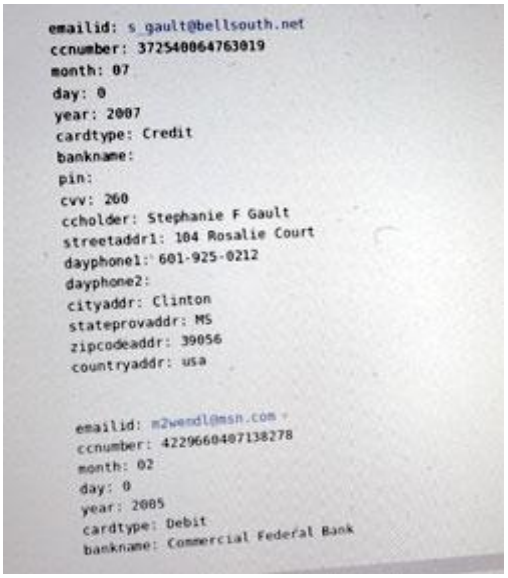
En un sondeo realizado entre personas con tarjetas de crédito con límites altos, todos negaron haber sido víctimas alguna vez de cobros indebidos. Pero sí afirmaron que las instituciones emisoras de sus tarjetas se han comunicado con ellos para informarles que, "por razones de seguridad", los números de sus cuentas serán modificados, y dijeron que enseguida les otorgaron uno nuevo, y que luego recibieron por correo a domicilio sus nuevas tarjetas. También comentaron que ya los han llamado para preguntarles si han hecho compras fuera de El Salvador con sus tarjetas, cuando ni siquiera han salido del país.

Estos relatos validan la versión de Pamela, quien trabaja en el área de seguridad informática bancaria y a cambio de su declaración pide el anonimato. Ella se suma a la afirmación de Funes acerca de la factibilidad de que un hacker pueda violar redes de seguridad.

Pamela asegura que ya ha habido casos de fuga de información, e incluso robos de bases de datos de clientes no solo de tarjetas de crédito, sino también de cuentas bancarias, y cree que los bancos nunca van a hacer públicos estos casos, que califica de "penosos". Y añade lo que significaría para ellos un escándalo mediático por denuncias por cobros indebidos y además exorbitantes.

Para ella cabe la posibilidad de que las mismas emisoras de tarjetas de crédito absorben los golpes de los hackers, por miedo a la vergüenza pública de verse en la obligación de desnudar su débil seguridad informática: "¿Qué les conviene más a los bancos: perder $5,000 o $20,000 cada cierto tiempo porque los hackearon o perder toda su cartera de clientes por su mala seguridad?".

Se solicitó hablar con Néstor Landaverde, presidente del comité de seguridad de la Asociación Bancaria Salvadoreña (ABANSA), para que definiera la posición de las emisoras de tarjetas de crédito, pero nunca hubo una respuesta. Incluso el departamento de comunicaciones de ABANSA pidió la formulación de un cuestionario, que se aseguró sería completado por Landaverde; sin embargo, esa contestación nunca llegó.



Por encargo. El año pasado compró a un amigo en Estados Unidos un boleto para un juego de fútbol con el crédito de otra persona. Abajo, información de clientes de bancos de EUA que le envió otro hacker.

A costa de la pasividad de una Fiscalía sobrecargada de trabajo, el desinterés por el fenómeno de los hackers —indiscutibles protagonistas de la era multimedia— y la vulnerable seguridad informática de las instituciones privadas y estatales salvadoreñas, Carlos y sus amigos pueden continuar divirtiéndose, comprando lo que quieran por internet y hackeando los sitios que se les antoje.

En su casa, ya en la oscurana del inicio de la noche, el hacker da por finalizada la plática. Pero antes de retirarse se le hace una última pregunta: ¿Cuándo vas a detenerte? Piensa unos segundos mientras su mirada se va inclinando hacia el suelo, tratando de ver su titubeante pie derecho; y al fin habla, lento: "Por el momento, pienso seguir. Pero en verdad ya he pensado en detenerme, porque sé que es posible que ya me estén siguiendo la pista, y si llego a cometer una regada, puede ser que den de un solo conmigo".

Se despide, cortés; camina hacia la puerta principal y abre la puerta. Ahí asoma su cabeza y hace un paneo de su pasaje de izquierda a derecha; apenas sale por un momento, luego se vuelve a meter y se queda con medio cuerpo afuera. Se ajusta su gorra y se despide una última vez antes de cerrar la puerta y regresar con su primo. Tiene miedo.

HACKERS Y CRACKERS FAMOSOS

CRACKERS

DRAPER JOHN , "CAPTAIN CRUNCH "

En septiembre de 1970 John Draper, también conocido como Captain Crunch, descubre que el obsequio ofrecido en las cajas de cereal Captain Crunch duplica perfectamente la frecuencia de tono de 2600 hz. de una línea de WATS, permitiéndole hacer llamadas telefónicas gratis y la gran víctima era AT&T.

HOLLAND WAU Y WENERY STEFFEN

"Lo logramos, por fin... Sólo hay algo seguro, la infinita inseguridad de la seguridad". Fue lo que escribio Wau Holland, en su cuaderno de notas, el 2 de mayo de 1987. Los dos hackers alemanes, de 23 y 20 años respectivamente, habían ingresado sin autorización al sistema de la central de investigaciones aerospaciales más grande del mundo (NASA).

¿Por qué lo hicieron?, "Porque es fascinante, la única aventura posible está en la pantalla de un ordenador", respondieron.

Cuando Wau y Steffen advirtieron que los técnicos los habían detectado, le enviaron un telex, avisando de su intrusión.

ING -HOU CHEN

Taipei, Taiwan, Abril 30 de 1999. El autor del virus "Chernobyl", dijo a los investigadores que el creó el bug con la esperanza de humillar y vengarse de los que llamo "proveedores incompetentes de antivirus para software". Pero él admitió que no esperaba que CIH (iniciales de su autor) causara daño alrededor del mundo. Este virus devastó cientos de miles de computadoras alrededor del mundo.

Chen creó el virus en Abril, cuando todavía era estudiante de ingeniería computacional en el Instituto Tecnológico.

Este inusual virus destructivo, programado para funcionar el 26 de Abril, (13° aniversario del desastre nuclear de Chernobyl), trata de borrar el disco rígido y escribir "basura" en algunos otros componentes, evitando de este modo el futuro encendido de la computadora.

KEVIN Y RONALD

Ronald y Kevin, con los nombres de guerra Makaveli y TooShort en el ciberespacio, asaltaron los ordenadores del Pentágono en Marzo del año 1998, a la tierna edad de 17 años. Estos dos forajidos virtuales, con sus conocimientos y con un equipo básico informático, se introdujeron en cuatro sistemas de la Marina y siete de las fuerzas aéreas, relacionados con centros digitales en Estados Unidos y Okinawa.

LA MACCHIA DAVID

En 1994 David La Macchia, estudiante de 20 años del prestigioso y serio MIT, reconoce que ha distribuido en Internet multitud de programas informáticos obtenidos sin licencia y por valor de un millón de dólares. Para ofrecerlos a los cibernautas montó su propia BBS.

LEVIN VLADIMIR

Un matemático ruso de 24 años, penetró vía Internet desde San Petersburgo en los sistemas informáticos centrales del banco Citybank en Wall Street, Este pirata logró transferir a diferentes cuentas de EE.UU., Rusia, Finlandia, Alemania, Israel, Holanda y Suiza fondos por valor de 10 millones de dólares, según el FBI. Detenido en el Reino Unido a principios de 1995, Levin espera que los tribunales británicos se pronuncien sobre una demanda de extradición solicitada por EE.UU.

MITNICK KEVIN , "EL CÓNDOR " , "EL CHACAL DE LA RED "

Como hacker, la carrera de Mitnick tiene sus inicios en 1980 cuando apenas contaba 16 años y, obsesionado por las redes de computadoras, rompió la seguridad del sistema administrativo de su colegio, pero no para alterar sus notas, lo hizo "solo para mirar".

La primera vez que lo detuvieron fue en 1981 por robar manuales de la Pacific Telephone. La información robada tenía un valor equivalente a los 200 mil dólares y tuvo que cumplir una condena tres meses de cárcel y a un año bajo libertad condicional.

En 1983 intentó ingresar en las computadoras de la universidad de California del Sur y poco después penetró el sistema de la agencia de créditos TRW.

En 1987 lo condenaron a treinta y seis meses de libertad condicional por robo de soft, tras hackear los sistemas del Departamento de Defensa de EE.UU. y la NASA.

Un año más tarde fue arrestado de nuevo cuando era estudiante de la Universidad del Sur de California. En esta ocasión entró ilegalmente a ARPAnet (la predecesora de Internet) y trató de acceder a la computadora del Pentágono. Lo sentenciaron a seis meses de cárcel en una prisión juvenil en California.

Durante ese tiempo le negaron el acceso a los teléfonos y a lo largo de los doce meses de rehabilitación no pudo acercarse a una computadora.

Más tarde, y ya en libertad, se apoderó de 16 códigos de seguridad de MCI y junto a un amigo, Lenny DiCicco, entraron a la red del laboratorio de investigaciones de Digital Corporation, conocida como Easynet.

Ambos hackers querían obtener una copia del prototipo del nuevo sistema operativo de seguridad de Digital llamado VMS. El personal de seguridad de Digital se dio cuenta inmediatamente del ataque y dieron aviso al FBI, y comenzaron a rastrear a los hackers.

Mitnick fue arrestado en 1988 por invadir el sistema de Digital Equipment. La empresa acusó a Mitnick y a DiCicco ante un juez federal de causarles daños por 4 millones de dólares en el robo de su sistema operativo. Fue declarado culpable de un cargo de fraude en computadoras y de uno por posesión ilegal de códigos de acceso de larga distancia.

Adicional a la sentencia el fiscal obtuvo una orden de la corte que prohibía a Mitnick el uso del teléfono en la prisión alegando que el prisionero podría obtener acceso a las computadoras a través de cualquier teléfono. A petición de Mitnick el juez lo autorizó a llamar únicamente a su abogado, a su esposa, a su madre y a su abuela y sólo bajo supervisión de un oficial de la prisión.

Este caso produjo revuelo en los Estados Unidos, no sólo por el hecho delictivo sino por la táctica que utilizó la defensa. Su abogado convenció al juez que Mitnick sufría de una adicción por las computadoras equivalente a la de un drogadicto, un alcohólico o un apostador. Gracias a esta maniobra de la defensa Mitnick fue sentenciado a sólo un año de prisión y al salir de allí debía seguir un programa de seis meses para tratar su "adicción a las computadoras". Durante su tratamiento le fue prohibido tocar una computadora o un módem y llegó a perder más de 45 kilos.

Para 1991 ya era el hacker que había ocupado la primera plana del New York Times y uno de sus reporteros, John Markoff, decidió escribir un libro de estilo Cyberpunk narrando las aventuras de Mitnick. Al parecer a Mitnick no le gustó el libro ya que luego de salir a la venta, la cuenta en Internet de Markoff fue invadida, cambiando su nivel de acceso, de manera de que cualquier persona en el mundo conectada a Internet podía ver su correo electrónico.

En 1992, y luego de concluir su programa, Mitnick comenzó a trabajar en una agencia de detectives. Pronto se descubrió un manejo ilegal en el uso de la base de datos y fue objeto de una investigación por parte del FBI quien determinó que había violado los términos de su libertad condicional. Se ofreció una recompensa de 1 millón de dólares a quien arrestara a Mitnick.

Luego de convertirse en prófugo de la justicia cambió de táctica y concluyó que la mejor manera de no ser rastreado era utilizando teléfonos celulares.

Luego de varios intentos infructuosos, en cuanto a calidad de información, se encontró con la computadora de Tsutomu Shimomura la cual invadió en la Navidad de 1994. Shimomura, físico computista y experto en sistemas de seguridad del San Diego Supercomputer Center, era además un muy buen hacker, pero era de los "chicos buenos", ya que cuando hallaba una falla de seguridad en algún sistema lo reportaba a las autoridades, no a otros hackers.

Shimomura notó que alguien había invadido su computadora en su ausencia, utilizando un método de intrusión muy sofisticado y que él nunca antes había visto. El intruso le había robado su correo electrónico, software para el control de teléfonos celulares y varias herramientas de seguridad en Internet. Allí comenzó la cuenta regresiva para Mitnick. Shimomura se propuso como orgullo personal atrapar al hacker que había invadido su privacidad.

Más tarde, El 16 de febrero de 1995, Mitnick fue capturado, juzado y condenado a 25 años de prisión, lejos de computadoras y teléfonos.

Pero, el 22 de marzo de 1999, se consigue un acuerdo con jueces y fiscales. Los términos concretos se desconocen, pero se sabe que en marzo de 2000 Mitnick quedaría en libertad con la condición irrevocable de no poder acercarse a una computadora.

Kevin Mitnick, este sencillo nombre, oculta la verdadera identidad de uno de los mayores crackers de la historia. Fue una de las mayores pesadillas del Departamento de justicia de los Estados Unidos. Entró virtualmente en una base de misiles, llegó a falsificar 20.000 números de tarjetas de crédito y a causar pérdidas millonarias a varias empresas.

MORRIS ROBERT

En noviembre de 1988, Morris lanzó un programa "gusano", diseñado por él mismo, buscando debilidades en sistemas de seguridad, y que pudiera correrse y multiplicarse por sí solo. La expansión exponencial de este programa causó el consumo de los recursos de y más de 6000 sistemas resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causo a las víctimas muchos días de productividad perdidos, y millones de dólares.

Como consecuencia, se creo el CERT (Equipo de Respuesta de Emergencias Computacionales) para combatir problemas similares en el futuro. Morris fue condenado y sentenciado a tres años de libertad condicional, 400 horas de servicio comunitario y US $10000 de fianza, bajo el cargo de Fraude computacional y abuso. La sentencia fue fuertemente criticada debido a que fue muy ligera, pero reflejaba lo inocuo de las intenciones de Morris más que el daño causado.

MURPHY IAN , "CAPTAIN ZAP "

En julio de 1981 Ian Murphy, un muchacho de 23 años que se autodenominaba "Captain Zap", gana notoriedad cuando entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.

En 1981, no había leyes muy claras para prevenir el acceso no autorizado a las computadoras militares o gubernamentales. "Captain Zap" mostró la necesidad de hacer mas clara la legislación. Con cargos de robo de propiedad, finalmente, Murphy fue multado por US$ 1000 y sentenciado a 2½ años de prueba.

"PAINT " Y "HAGIS "

Estos son los seudónimos de los dos hackers que el 10 de Diciembre de 1997 accedieron a uno de los buscadores mas utilizados en Internet. Los terroristas informáticos autodenominados "Paints & Hagis", accedieron al servidor del popular navegador Yahoo! y dejaron un mensaje amenazante a los casuales visitantes.

Este ataque no resultó ser más de una modificación de una página web, y un ejemplo temprano de las muchas que se modifican hoy día a día.

PETERSON JUSTIN TANNER , "AGENT STEAL "

Peterson crackeaba las agencias de crédito. Esta falta de personalidad le llevó a su caída y a la de otros. Tiempo después, se dice, obtuvo un trato con el FBI. Esto le facilitó su salida de la cárcel y "no" pudo ser demostrado un fraude mediante una trasferencia de dinero.

POULSEN KEVIN , "DARK DANTE "

En diciembre de 1992 Kevin Poulsen fue acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar americana. Se acusó Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y fue condenando a 10 años en la cárcel (salió bajo palabra a los 5 años).

Como Cracker, siguió el mismo camino que Kevin Mitnick, pero fue más conocido por su habilidad para controlar el sistema telefónico de Pacific Bell. Incluso llegó a "ganar" un Porsche en un concurso radiofónico, si su llamada fuera la 102, y así fue. Poulsen también crackeó todo tipo de sitios, pero él se interesaba por los que contenían material de defensa nacional. Esto fue lo que lo llevó a su estancia en la cárcel, 5 años, fue liberado en 1996, supuestamente "reformado".

SMITH DAVID

Programador de 30 años, detenido por el FBI y acusado de crear y distribuir el virus que ha bloqueado miles de cuentas de correo, "Melissa". Entre los cargos presentados contra él, figuran el de "bloquear las comunicaciones publicas" y de "dañar los sistemas informáticos". Acusaciones que en caso de demostrarse en el tribunal podrían acarrearle una pena de hasta 10 años de cárcel.

Por el momento y a la espera de la decisión que hubiese tomado el juez, David Smith esta en libertad bajo fianza de U$S 10000. Melissa en su "corta vida" había conseguido contaminar a más de 100.000 computadoras de todo el mundo, incluyendo a empresas como Microsoft, Intel, Compaq, administraciones públicas estadounidenses como la del Gobierno del Estado de Dakota del Norte y el Departamento del Tesoro.

Sin embargo, la detención de Smith no significa que el virus haya dejado de actuar. Compañías informáticas siguen alertando que aún pueden quedar miles de usuarios expuestos a sus efectos, por desconocimiento o por no haber instalado en sus equipos sistemas antivíricos que frenen la actividad de Melissa u otros virus, que han venido apareciendo últimamente como Happy99 o Papa.

THE MENTOR Y GRUPO H 4 G 1 3

El autodenominado grupo H4G13, con Mentor a su cabeza quería demostrar hasta donde eran capaces de llegar, y lo dejaron plasmado de una manera efectiva, colocando en la pagina principal de la NASA, durante media hora, el "manifiesto" hacker más conocido hasta el momento. Ver Capítulo 5.

ZINN HERBERT , "SHADOWHACK "

Herbert Zinn, (expulsado de la educación media superior), y que operaba bajo el seudónimo de "Shadowhawk", fue el primer sentenciado bajo el cargo de Fraude

Computacional y Abuso. Zinn tenia 16 cuando violó el acceso a AT&T y los sistemas del Departamento de Defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US$ 174000 en archivos, copias de programas, los cuales estaban valuados en millones de dólares, además publico contraseñas y instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y a una fianza de US$ 10000.

HACKERS

ARDITA JULIO CESAR , "EL GRITÓN "

Es considerado el hacker más famoso de Argentina. Nació en Río Gallegos, el 28 de marzo del 1974. Utilizó su primera computadora mientras realizaba su secundaria. En quinto año, junto con dos compañeros ayudaron a informatizar el sistema de notas y facturación del colegio en el cual estudiaba.

Este muchacho, saltó a la fama el 28 de diciembre de 1995, día de los Santos Inocentes, cuando su domicilio fue allanado por la Justicia Argentina luego de que los Estados Unidos alertaran sobre reiteradas intrusiones a varias de sus redes informáticas de Defensa, entre ellas la del Pentágono.

Las intrusiones provenían de una computadora conectada a una línea telefónica desde un departamento de Barrio Norte, en la Capital Federal. "El Gritón" ingresaba en la red de computadoras de la empresa Telecom a través de líneas gratuitas 0800, para luego realizar intromisiones en sistemas informáticos ajenos.

En la causa argentina número 45048/95, con carátula "Ardita Julio C., sobre defraudación", el juzgado de Instrucción número 38 a cargo de la jueza Wilma López, dispuso que Ardita compareciera ante un tribunal oral pero por fraude telefónico (estimado por la empresa Telecom en $50), ya que las intrusiones informáticas no están contempladas en el Código Penal.

Sin embargo, por el mismo episodio, Ardita ya tuvo que recorrer una espinosa demanda penal en los Estados Unidos, donde las intrusiones informáticas, las violaciones de códigos secretos y la posesión de claves ajenas sí son delitos graves. El proceso terminó el 19 de mayo 1999, cuando un tribunal de la ciudad de Boston, lo condenó a 3 años de libertad condicional y a pagar una multa de U$S5000 por haber vulnerado, entre otros varios, el sistema informático de la Marina.

Hoy en día, con 27 años, Julio Cesar Ardita paga religiosamente sus facturas telefónicas; se levanta temprano por las mañanas y camina hasta la zona de Tribunales. Allí está Cybsec S.A., la exitosa empresa de seguridad informática que el ex-Gritón administra junto a su socio.

BARAM PAUL

Posiblemente el mayor hacker de la historia. Ya hackeaba Internet antes de que existiera. El fué quien introdujo el concepto de hacker.

FARMER DAN

Trabajó con Spafford en la creación de COPS (1991) y al mismo tiempo con el famoso Computer Emergency Response Team (CERT). Tiempo más tarde Farmer ganó gran notoriedad al crear el System Administrator Tool for Analyzing Networks (SATAN). Una gran herramienta para analizar vulnerabilidades en redes.

GATES BILL Y ALLEN PAUL

En sus tiempos de aprendices, estos dos hombres de Washington se dedicaban a hackear software. Empezaron en los 80 y han creado los mayores imperios de software de todo el mundo.

RITCHIE DENNIS , THOMSON KEN Y KERRIGHAN BRIAN

Programadores de los Laboratorios Bell. Son los desarrolladores de UNIX y C. Se los considera los padres de la informática masiva al desarrollar el sistema operativo y el lenguaje más poderosos de la actualidad.

SPAFFORD EUGENE

Profesor de informática. Colaboró para crear el Computer Oracle Password Security System (COPS) un sistema de seguridad semiautomático. Es un hombre muy respetado en el campo de la seguridad.

STALLMAN RICHARD

Se unió al Laboratorio de inteligencia artificial de la MIT en 1971. Fue ganador del premio McArthur por sus desarrollos de software. Fue fundador de Free Software Foundation, creando aplicaciones y programas gratis.

TORVALDS LINUS

Torvalds empezó a conocer el UNIX y a tomar clases de programación en C sobre los 90. Un año después empezó a escribir un SO parecido al UNIX. Después de otro año, lo subió a Internet pidiendo colaboración; hoy es llamado LINUX.

VEHEMA WIETSE

Vehema viene de la Universidad de Tecnología de Eindhoven, en los Países Bajos. Un gran programador, con un don para ello, además de tener un amplio historial en programas sobre seguridad. Es el coautor del SATAN con Farmer. Vehema escribió el TCP Wrapper, uno de los programas de seguridad más usado en el mundo.

Instituto Nacional
de Tecnologías
de la Comunicación

CONSEJOS GENERALES DE SEGURIDAD

Internet y los menores:

1. Eduque al menor sobre los posibles peligros que puede encontrar en la Red.
2. Acompañe al menor en la navegación cuando sea posible, sin invadir su intimidad.
3. Advierta al menor de los problemas de facilitar información personal (nombre, dirección, teléfono, contraseñas, fotografías, etc.) a través de cualquier canal.
4. Desaconséjele participar en charlas radicales (provocadoras, racistas, humillantes, extremistas, etc.) ya que pueden hacerle sentir incómodo.
5. Infórmele de que no todo lo que sale en Internet tiene que ser cierto, ya que pueden ser llevados a engaño con facilidad.
6. Preste atención a sus 'ciber-amistades' en la misma media que lo hace con sus amistades en la vida real.
7. Pídale que le informe de cualquier conducta o contacto que le resulte incómodo o sospechoso.
8. Vigile el tiempo de conexión del menor a Internet para evitar que desatienda otras actividades.
9. Utilice herramientas de control parental que le ayudan en el filtrado de los contenidos accesibles por los menores.
10. Cree una cuenta de usuario limitado para el acceso del menor al sistema.

Redes P2P:

1. Analice todos los archivos que se descargue a través de las redes de intercambio de ficheros.
2. No comparta software ilegal ya que incurriría en un delito.
3. Ejecute el cliente P2P en una sesión de usuario con permisos limitados para aislarlo de otros componentes críticos del sistema.
4. Modifique el nombre de las carpetas de descarga ya que muchos códigos maliciosos buscan rutas fijas para replicarse.
5. Preste atención a la extensión de los ficheros que descarga, podrían indicar amenazas (por ejemplo, una imagen nunca tendrá extensión .exe).

Dispositivos móviles:

1. Desactive el bluetooth o infrarrojos mientras no los vaya a utilizar.
2. Configure el dispositivo en modo oculto, para que no pueda ser descubierto por atacantes.
3. No acepte conexiones de dispositivos que no conozca para evitar transferencias de contenidos no deseados.
4. Instale un antivirus y manténgalo actualizado para protegerse frente al código malicioso.
5. Ignore / borre SMS o MMS de origen desconocido que inducen a descargas o accesos a sitios potencialmente peligrosos.
6. Active el acceso mediante PIN (al bluetooth y al móvil) para que sólo quién conozca este código pueda acceder a las funcionalidades del dispositivo.
7. Bloquee la tarjeta SIM en caso de pérdida para evitar que terceros carguen gastos a su cuenta.
8. No descargue software de sitios poco fiables o sospechosos para impedir la entrada por esta vía de códigos potencialmente maliciosos.
9. Lea los acuerdos de usuario del Sw que instala por si se advierte de la instalación de componentes no deseados (software espía).

Juegos en línea:

1. Evite compartir usuario / contraseña tanto dentro como fuera de la plataforma del juego.
2. Actualice el software del juego para evitar fallos de seguridad conocidos.
3. No adquiera créditos en páginas de subastas en línea sin que estén certificados por los creadores del juego.
4. Vigile los movimientos de su cuenta/tarjeta bancaria si la tiene asociada al juego, para detectar movimientos ilícitos.
5. Controle su tiempo de juego ya que esta actividad pueden ser muy adictivo

Wi-fi:

1. Fije un número máximo de equipos que se puedan conectar al punto de acceso.
2. Apague el punto de acceso cuando no vaya a utilizarlo.
3. Desactive la difusión de su SSID (nombre de su red wifi) para evitar que equipos externos identifiquen automáticamente los datos de su red inalámbrica.
4. Active el filtrado por dirección MAC para que sólo los dispositivos permitidos tengan acceso a la red.
5. Cambie la contraseña por defecto ya que muchos fabricantes utilizan la misma clave para todos sus equipos.
6. Utilice encriptación WPA (o WEP si su sistema no permite la primera), para impedir que el tráfico de red sea fácilmente legible. Se recomienda WPA ya que WEP es inseguro.
7. Desactive la asignación dinámica de IP (DHCP) a nuevos dispositivos que se quieran conectar a la red, haciéndose necesaria la asignación manual de las IPs.

Equipos portátiles:

1. No deje el portátil desatendido en lugares públicos para evitar que sea sustraído.
2. Utilice un candado físico para anclar el portátil cuando vaya a ausentarse temporalmente.
3. Cifre el contenido del portátil para evitar el acceso a los datos si el equipo es robado.
4. Elimine datos innecesarios que puedan estar almacenados en el portátil.

Banca en línea / Comercio electrónico:

1. Observe que la dirección comienza por httpS que indica que se trata de una conexión segura.
2. Observe que aparece un candado ( ) en la parte inferior derecha de su navegador.
3. Asegúrese de la validez de los certificados (pulsando en el candado), que coinciden con la entidad solicitada y sean vigentes y válidos.
4. Tenga en cuenta que su banco NUNCA le pedirá información confidencial por correo electrónico ni por teléfono.
5. Evite el uso de equipos públicos (cibercafés, estaciones o aeropuertos, etc) para realizar transacciones comerciales.
6. Desactive la opción 'autocompletar' si accede desde un equipo distinto al habitual o comparte su equipo con otras personas.
7. Cierre su sesión cuando acabe, para evitar que alguien pueda acceder a sus últimos movimientos, cambiar sus claves, hacer transferencias, etc.
8. Instale alguna herramienta de antifraude para evitar acceder a páginas fraudulentas.

Chat / Mensajería instantánea:

1. Evite invitaciones a visitar sitios web que le resulten sospechosas o que procedan de desconocidos.
2. Rechace ficheros adjuntos que no haya solicitado o que le parezcan sospechosos.
3. Tenga precaución al conversar o agregar contactos desconocidos.
4. No facilite datos confidenciales (contraseñas, nombres de usuario, datos bancarios, etc.) a través de estos canales.
5. Rechace los usuarios 'no deseados', de los que no quiera recibir mensajes.

Navegación:

1. No descargue/ejecute ficheros desde sitios sospechosos porque pueden contener código potencialmente malicioso.

2. Analice con un antivirus todo lo que descarga antes de ejecutarlo en su equipo.

3. Mantenga actualizado su navegador para que este protegido frente a vulnerabilidades con parche conocido.

4. Configure el nivel de seguridad de su navegador según sus preferencias.

5. Instale un cortafuegos que impida accesos no deseados a / desde Internet.

6. Descargue los programas desde los sitios oficiales para evitar suplantaciones maliciosas.

7. Utilice anti-dialers si navega con RTB o RDSI para evitar conectarse a Internet a través de números de tarificación adicional, que incrementarían su factura.

8. Puede utilizar mata-emergentes para eliminar las molestas ventanas emergentes (pop-up) que aparecen durante la navegación, o configurar su navegador para evitar estas ventanas.

9. Utilice un usuario sin permisos de Administrador para navegar por Internet, así impide la instalación de programas y cambios en los valores del sistema.

10. Borre las cookies, los ficheros temporales y el historial cuando utilice equipos ajenos (públicos o de otras personas) para no dejar rastro de su navegación.

SIEMPRE:

1. Manténgase informado sobre las novedades y alertas de seguridad.
2. Mantenga actualizado su equipo, tanto el Sistema Operativo como cualquier aplicación que tenga instalada.
3. Haga copias de seguridad con cierta frecuencia, para evitar la pérdida de datos importante.
4. Utilice software legal que le suelen ofrecer garantía y soporte.
5. Utilice contraseñas fuertes en todos los servicios, para dificultar la suplantación de su usuario (evite nombres, fechas, datos conocidos o deducibles, etc.).
6. Utilice herramientas de seguridad que le ayudan a proteger / reparar su equipo frente a las amenazas de la Red.
7. Cree diferentes usuarios, cada uno de ellos con los permisos mínimos necesarios para poder realizar las acciones permitidas

Correo electrónico:

1. No abra ficheros adjuntos sospechosos procedentes de desconocidos o que no haya solicitado.
2. Utilice un filtro anti-spam para evitar la recepción de correo basura.
3. Analice los anexos con un antivirus antes de ejecutarlos en su sistema.
4. Desactive la vista previa de su cliente de correo para evitar código malicioso incluido en el cuerpo de los mensajes.
5. No facilite su cuenta de correo a desconocidos ni la publique 'alegramente'.
6. No responda a mensajes falsos, ni a cadenas de correos para evitar que su dirección se difunda.
7. Borre el historial de destinatarios cuando reenvíe mensajes a múltiples direcciones

ANEXO XII

GOBIERNO DE TI A TRAVÉS DE ITIL Y COBIT

Fernando Chimeno

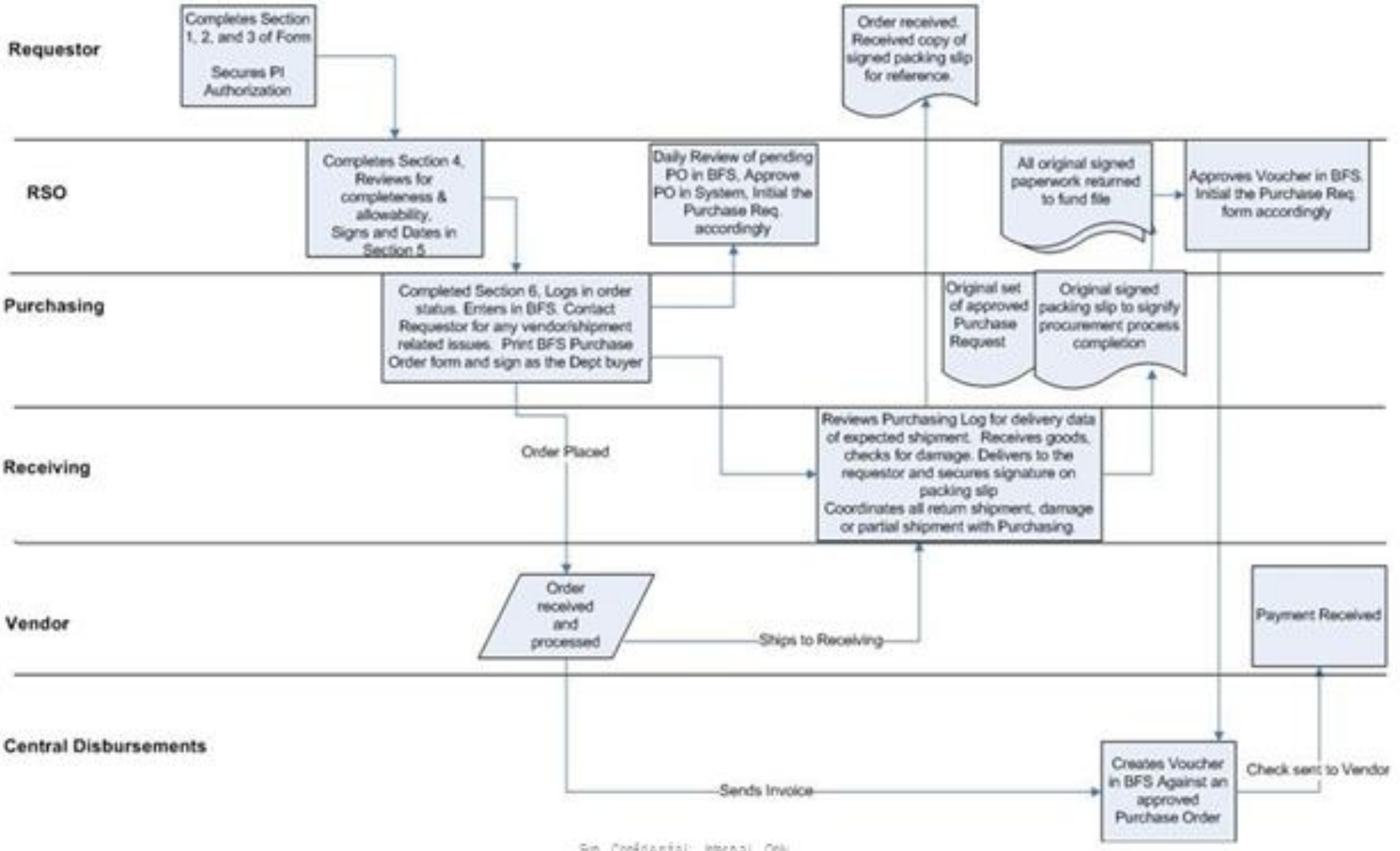
Consultant

Educational Services

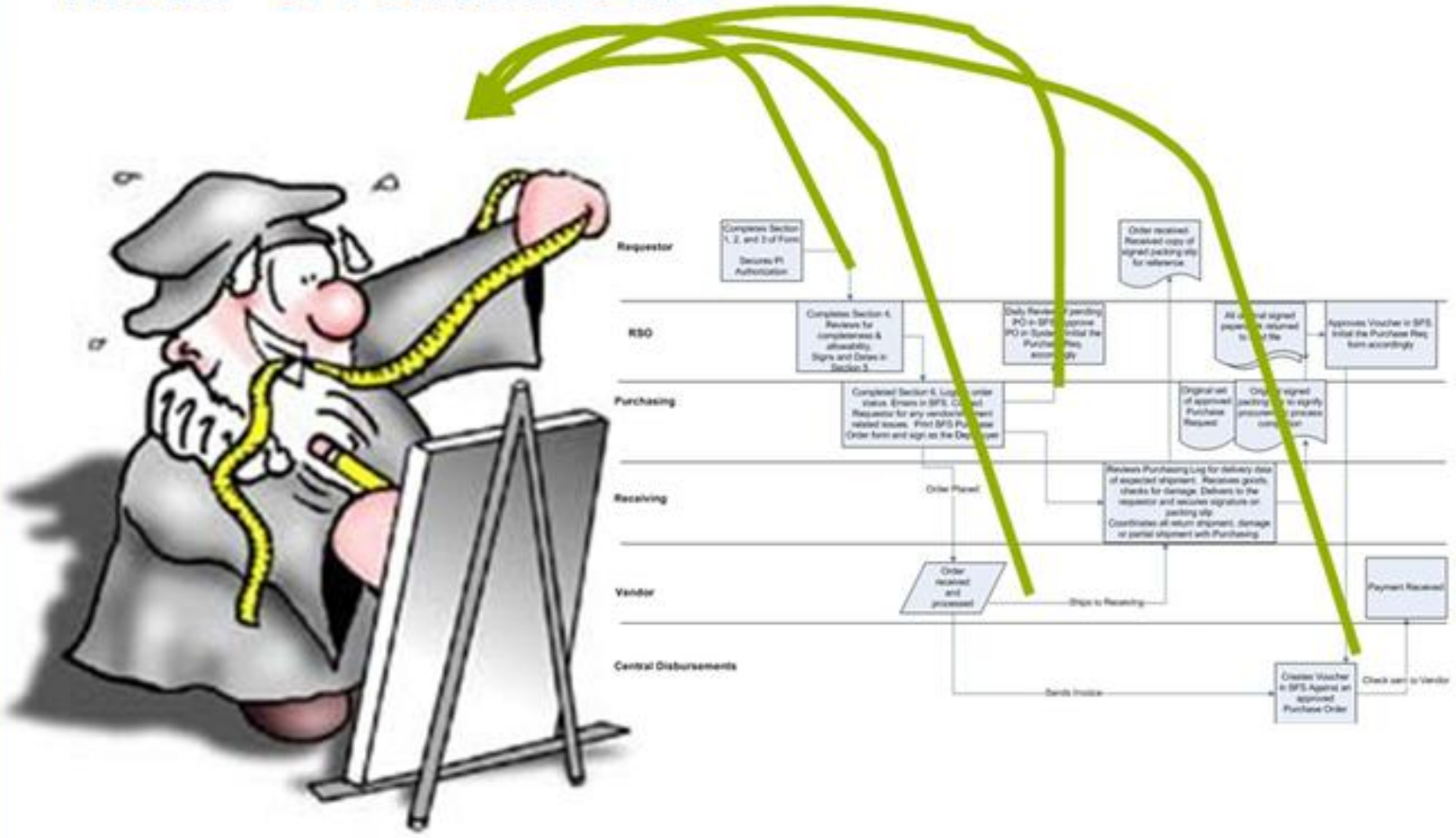
Sun Microsystems, Iberia

Control de TI: CobiT y BSC

¿Cual es el siguiente paso?



Medir el rendimiento



¿Qué medidas interesan?

Tecnología

cambios realizados con éxito

de violaciones de acceso

Frecuencia de las revisiones de rendimiento y capacidad

Negocio

contratos cancelados por interrupciones del servicio

incidentes de seguridad con impacto sobre imagen pública

de procesos de negocio no cubiertos por un plan de disponibilidad

CobiT

"Para proporcionar la información que necesita la compañía para alcanzar sus objetivos, es necesario gestionar y controlar los recursos de TI utilizando un conjunto estructurado de procesos, y así entregar los servicios de información necesarios"

Misión

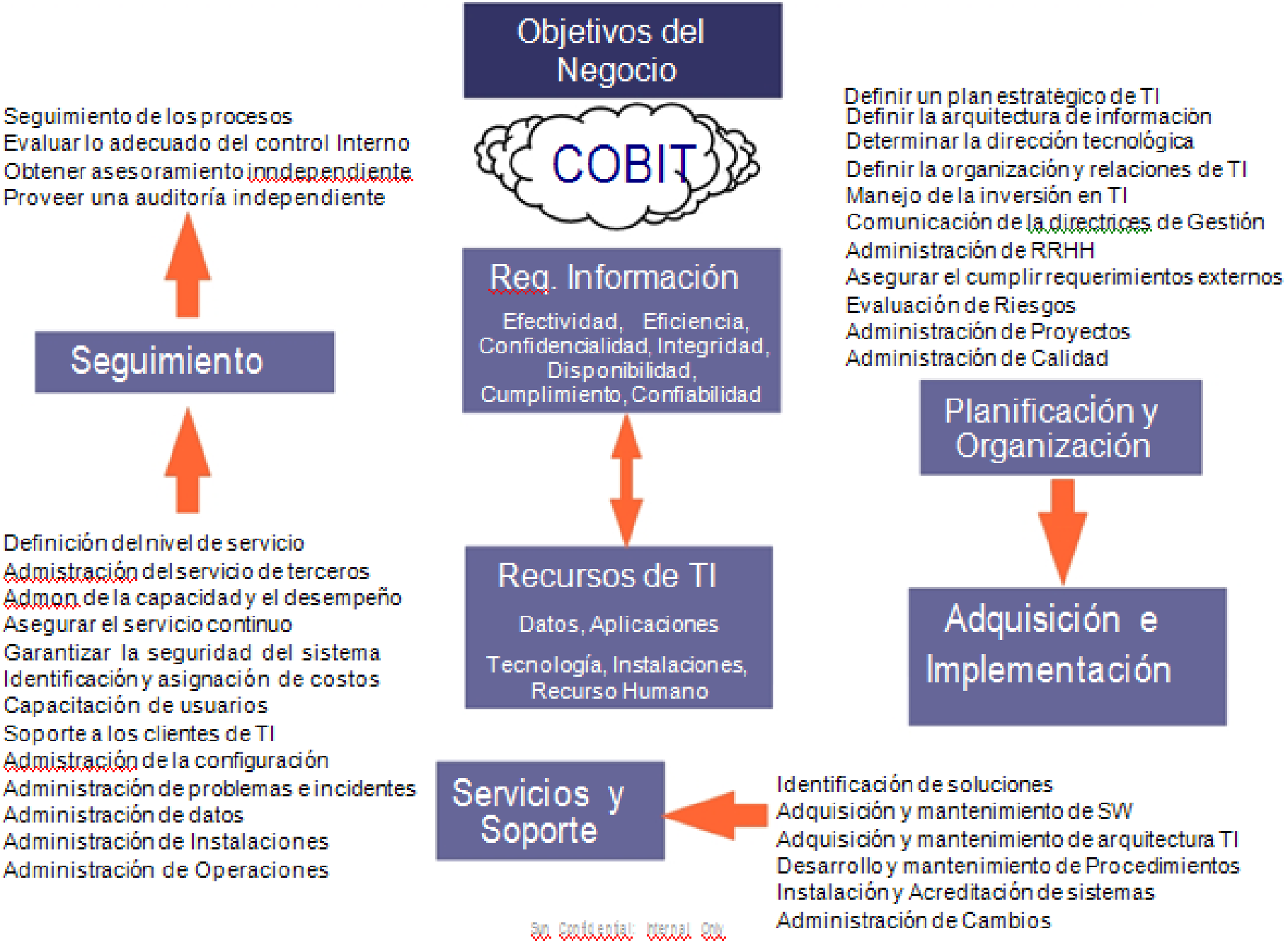
Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes, auditores..

¿Qué es Cobit?

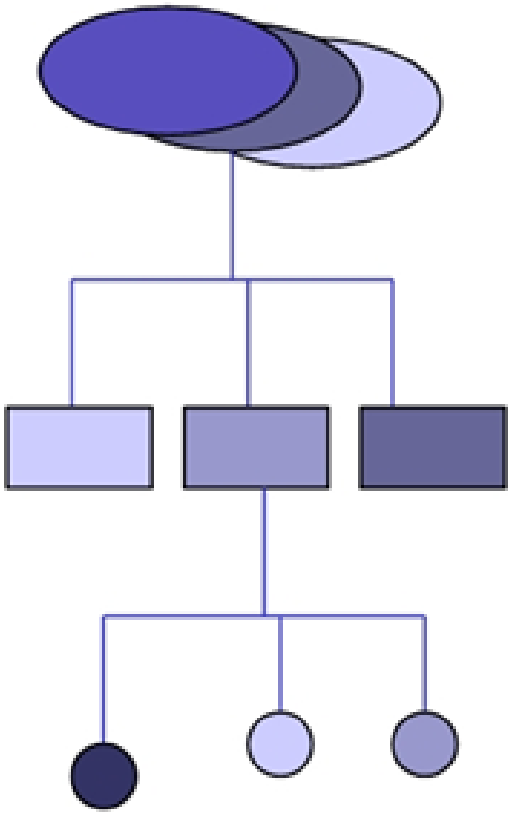
- Control Objectives for Information and related Technology.
- Set de documentación.
- Marco Referencial para la gestión de TI.
- Control y métricas de TI, no especifica un framework específico a nivel de operaciones
- Define KGIs, KPIs, SFs y fija BSC de los procesos de tecnología.

¿Qué es Cobit?

- Integra y concilia normas y reglamentaciones existentes como:
  - > ISO (9000-3)
  - > Códigos de Conducta del Consejo Europeo
  - > COSO, IFAC, IIA, ISACA, AICPA y Otras
- 1ª Edición Septiembre de 1996
- 2ª Edición Abril de 1998
- 3ª Edición Marzo de 2000
- 4ª Edición Noviembre 2005



Niveles de Gestión



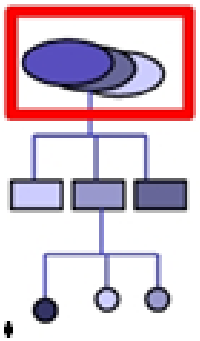
Dominios: Agrupación Natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional

Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control.

Tareas: Acciones requeridas para lograr un resultado medible. Las Actividades

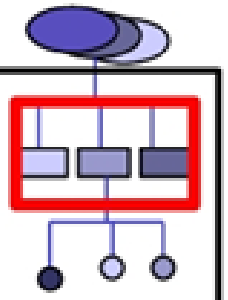
Tienen un ciclo de vida mientras que las tareas son discretas.

Dominios Cobit



- **Planificación y Organización:** Estrategia y Táctica, alineacion con los Objetivos de Negocio.
- **Adquisición e Implementación:** Identificación, Desarrollo/ Adquisicion, Cambios y Mantenimiento.
- **Entrega y Soporte:** Entrega de Servicios, Training, Procesos de Soporte.
- **Monitorización:** Verificación de Calidad y Capacidad.

Procesos Cobit



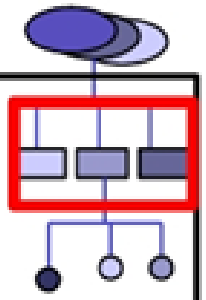
Planificación y Organización

- Definir un plan estratégico de TI
- Definir la arquitectura de información
- Determinar la dirección tecnológica
- Definir la organización y relaciones de TI
- Manejo de la inversión en TI
- Comunicación de la directrices Gerenciales
- Administración del Recurso Humano
- Asegurar el cumplir requerimientos externos

Adquisición e Implementación

- Evaluación de Riesgos
- Administración de Proyectos
- Administración de Calidad
- Desarrollo y mantenimiento de Procedimientos de TI
- Instalación y Acreditación de sistemas
- Administración de Cambios

Procesos Cobit



Entrega y Soporte

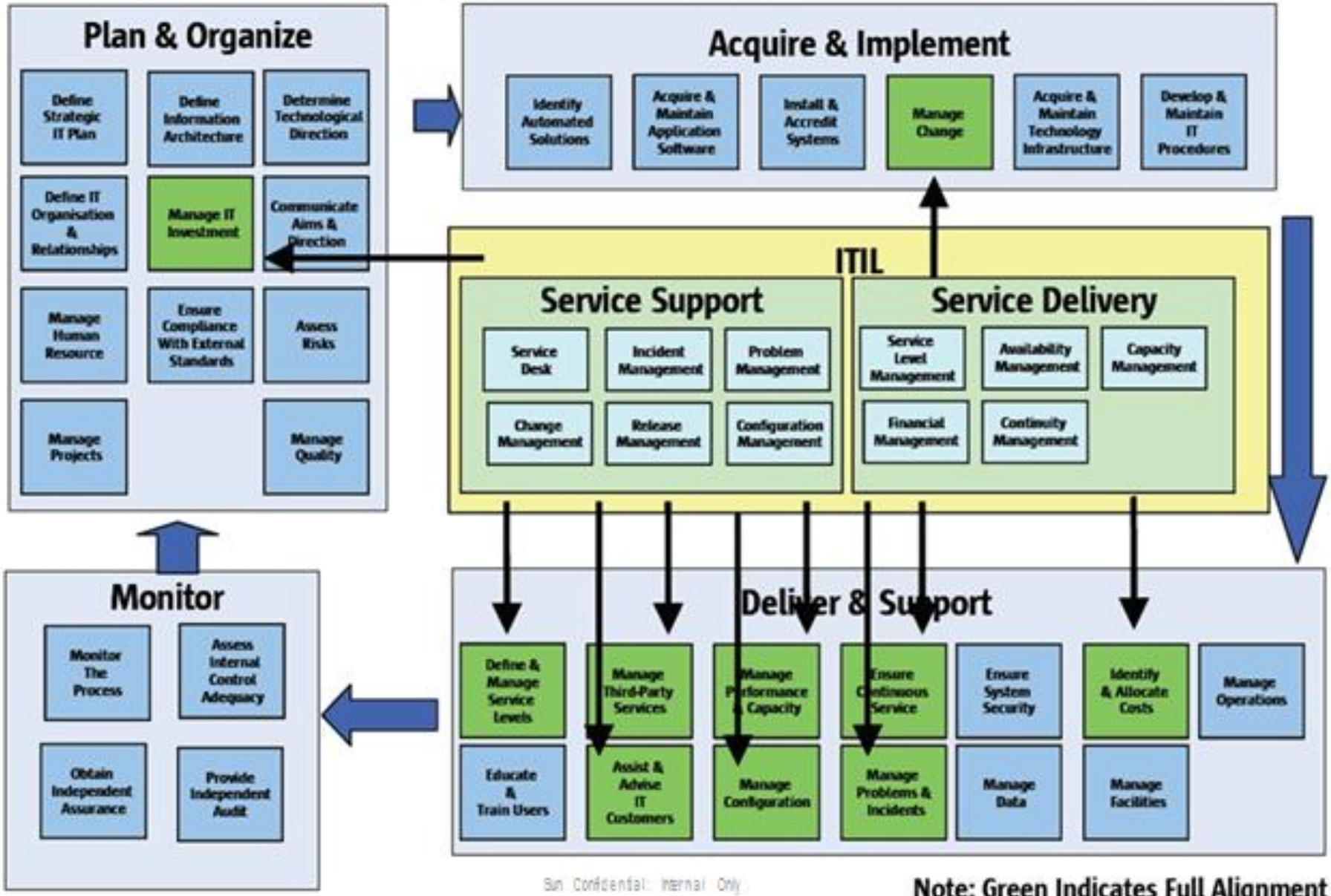
- Definición del nivel de servicio
- Admistración del servicio de terceros
- Admon de la capacidad y el desempeño
- Asegurar el servicio continuo
- Garantizar la seguridad del sistema
- Identificación y asignación de costos
- Capacitación de usuarios
- Soporte a los clientes de TI
- Admistración de la configuración
- Administración de problemas e incidentes

Monitorización

- Seguimiento de los procesos
- Evaluar lo adecuado del control Interno
- Obtener aseguramiento independiente

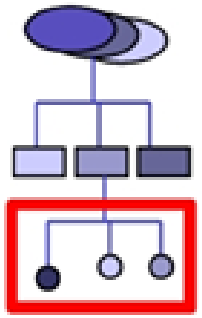
- Proveer una auditoria independiente

Mapping ITIL y Cobit



Note: Green Indicates Full Alignment

Indicadores Cobit

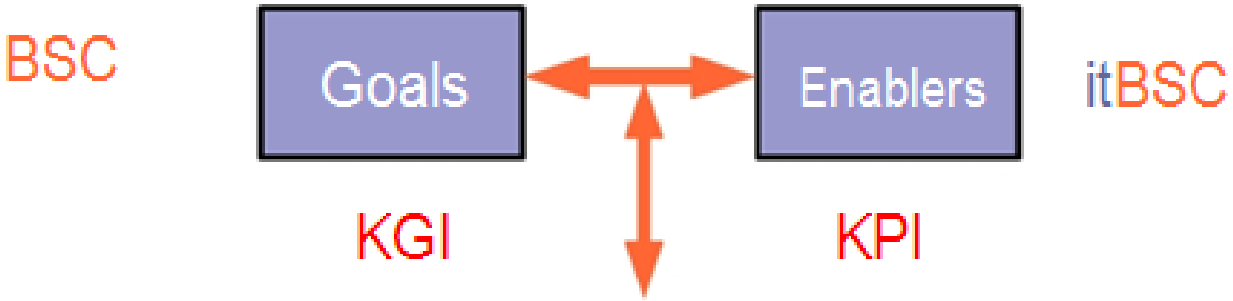


- KEY GOAL INDICATOR

Objetivos de cada Proceso, es una medida de "qué" se tiene que alcanzar. Es un "target reflejo" del objetivo.

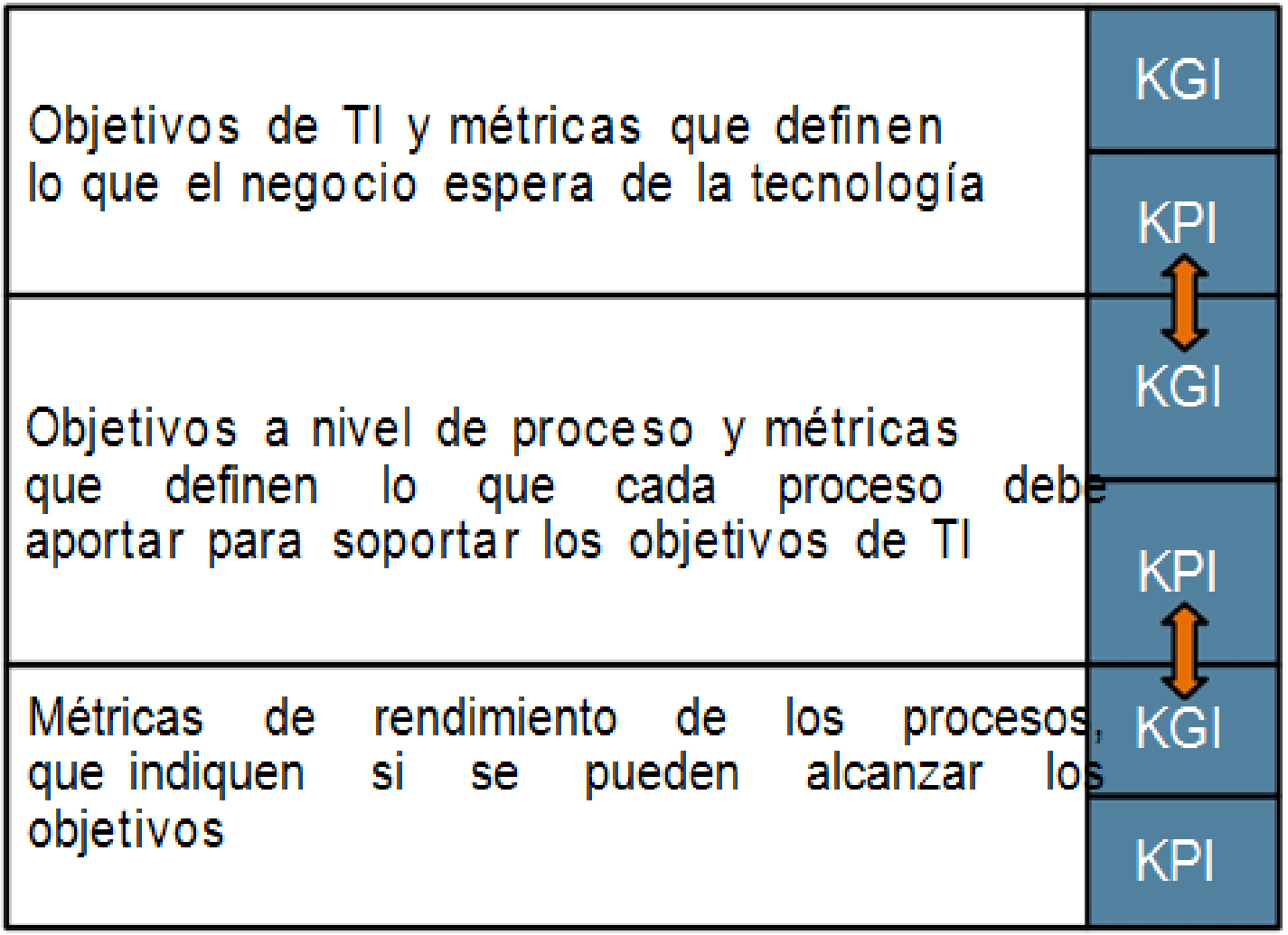
- KEY PERFORMANCE INDICATOR

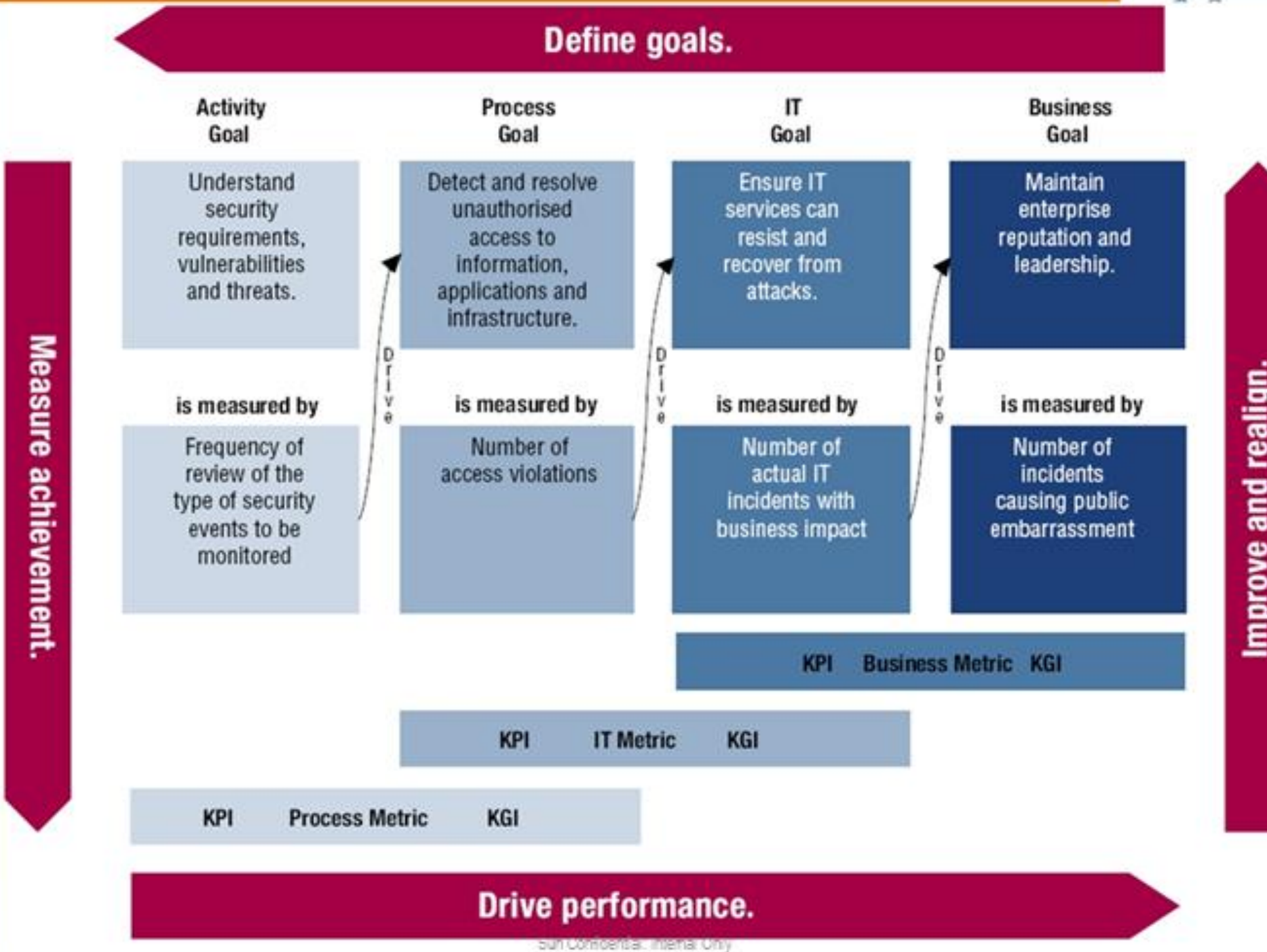
Son medidas que indican "cómo" se estan alcanzando los objetivos del proceso. "Enablers".



Eficiencia, Efectividad, Confidencialidad, Integridad, Disponibilidad, Conformidad, Fiabilidad

Niveles de medida




Define goals.
Activity Goal
Process Goal
IT Goal
Business Goal
Understand security requirements, vulnerabilities and threats.
Detect and resolve unauthorised access to information, applications and infrastructure.
Ensure IT services can resist and recover from attacks.
Maintain enterprise reputation and leadership.
Drive
Drive
Drive
is measured by
is measured by
is measured by
is measured by
Frequency of review of the type of security events to be monitored
Number of access violations
Number of actual IT incidents with business impact
Number of incidents causing public embarrassment
KPI Business Metric KGI
KPI IT Metric KGI
KPI Process Metric KGI
Measure achievement.
Improve and realign.
Drive performance.

Eficiencia de los indicadores

- Un buen ratio información/esfuerzo
- Deben ser comparables internamente, frente a valores históricos
- Deben ser comparables externamente, conindependencia de tamaño de la compañía o del sector
- Es mejor tener pocos indicadores buenos, que una lista interminable de ellos
- Deben ser fáciles de medir, y no deben confundirse con los objetivos

Construcción de los indicadores

- Una vez seleccionados los indicadores relevantes, ¿cómo podemos asegurar que las mediciones son buenas?

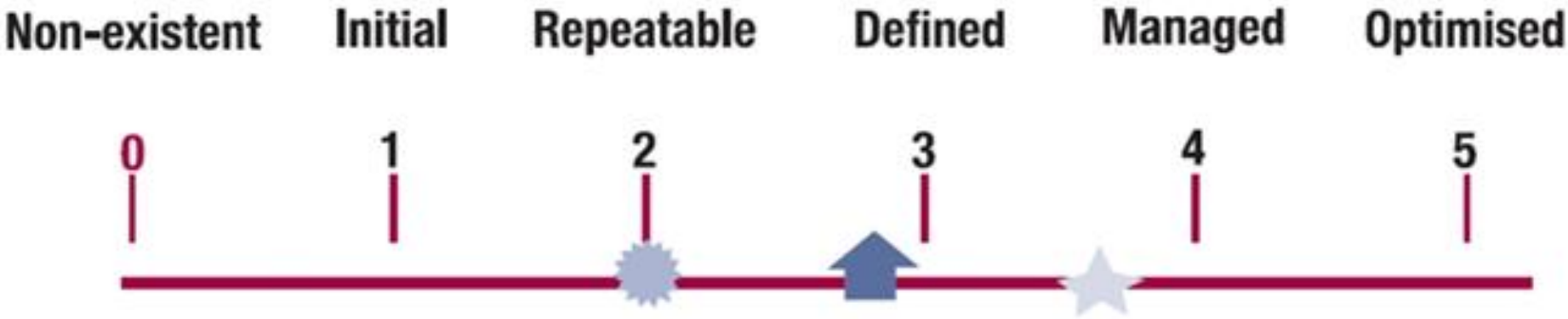
  > Se necesita un marco de procesos definido. A mayor madurez, más exactitud en las repeticiones

  > Se necesitan herramientas que den soporte a los indicadores

- ¿Cómo construimos los indicadores de negocio?

A través de indicadores de niveles inferiores

Modelo de Madurez



LEGEND FOR SYMBOLS USED

- Enterprise current status
- Industry average
- Enterprise target

LEGEND FOR RANKINGS USED

0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicate
4—Processes are monitored and measured.
5—Good practices are followed and automated.

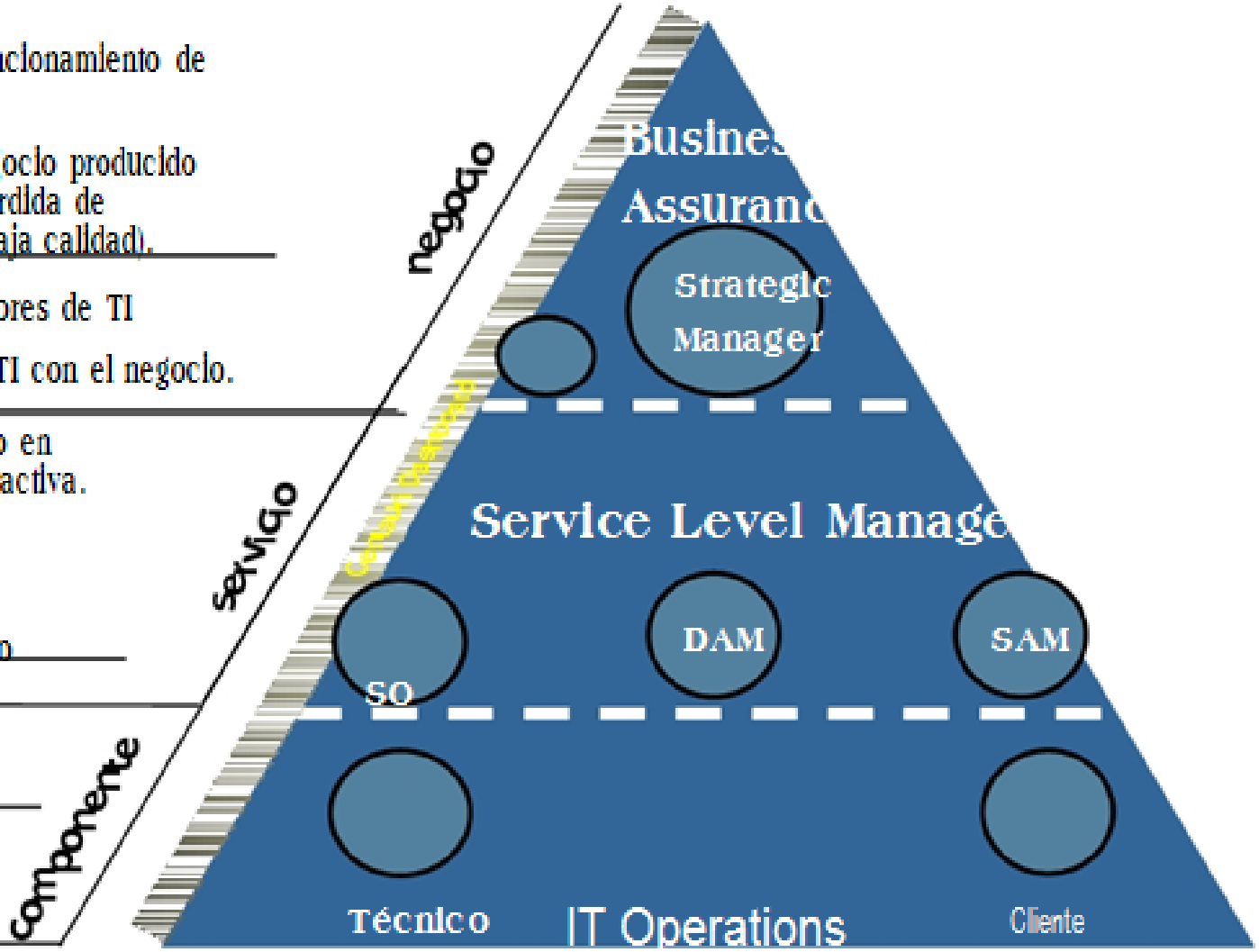
Diferentes Visiones de Servicio

- Conocer en tiempo real el funcionamiento de los procesos de negocio.
- Conocer el impacto en el negocio producido por pérdidas de servicio (pérdida de productividad, coste de la baja calidad).
- Mejor gestión de los proveedores de TI
- Asegurar el alineamiento de TI con el negocio.

- Gestión de niveles de servicio en tiempo real y de manera proactiva.
- Localización clara de responsabilidades.
- Control de Calidad de Servicio

- Correlación de eventos
- Resolución de problemas.

- Impacto en el negocio.
- Priorizar las respuestas.



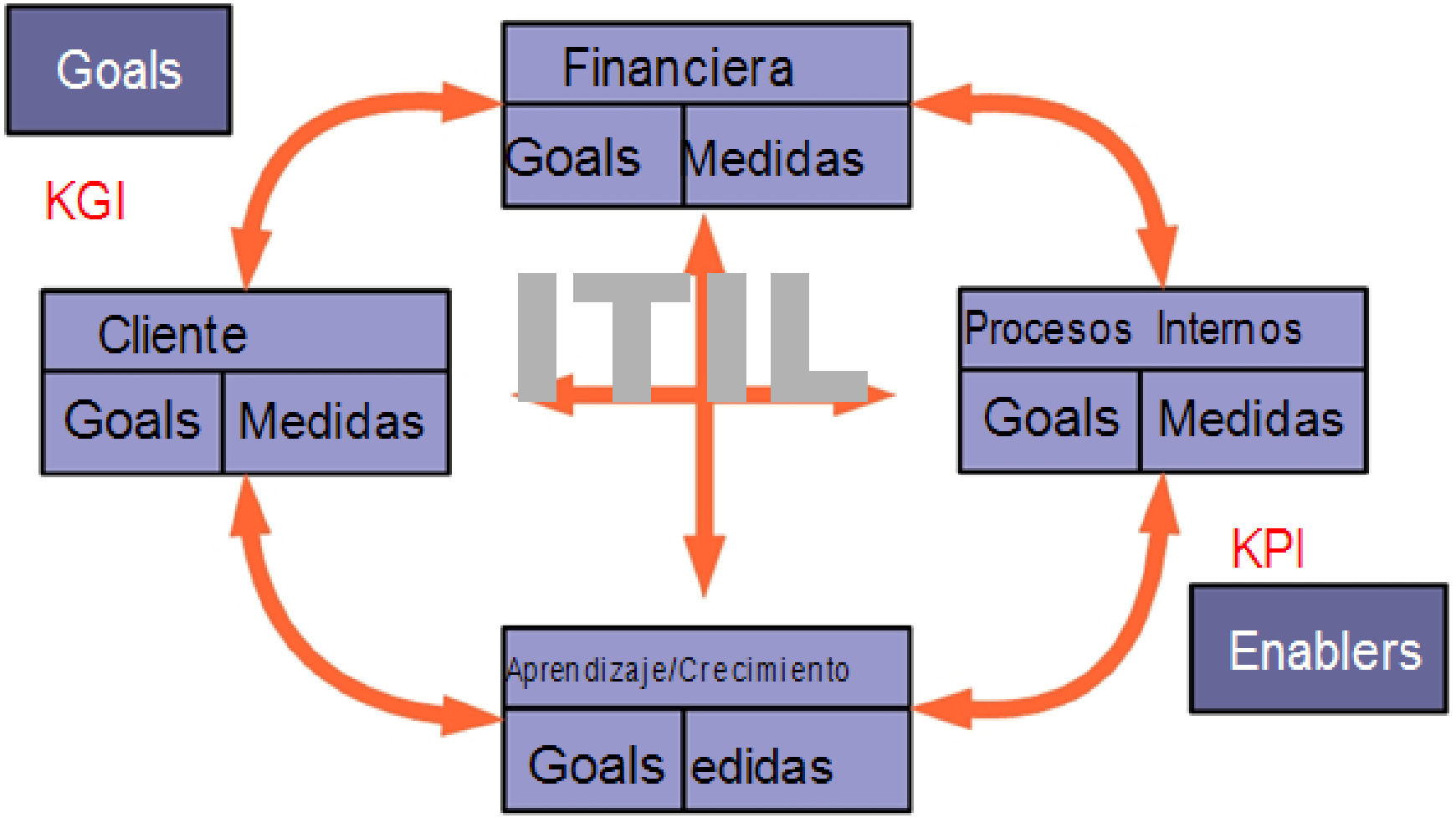
BSC: Balance ScoreCard

"Una seria deficiencia en los sistemas de gestión tradicionales: su incapacidad para unir la estrategia de largo plazo de la empresa con sus acciones de corto plazo".

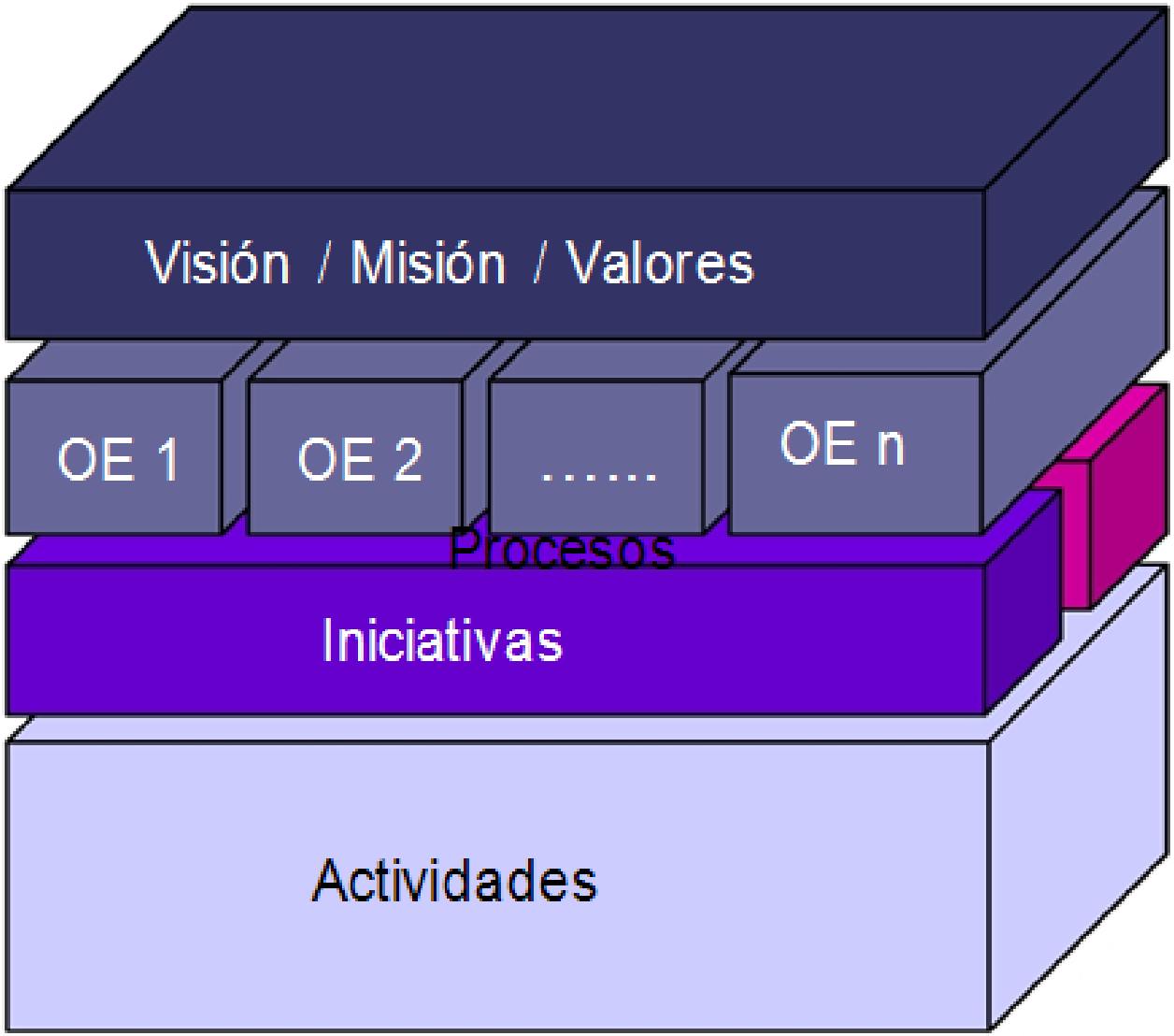
Robert S. Kaplan / David P. Norton
"Balance Scorecard, Traslating strategy in action"

BSC: Balance ScoreCard para TI

Primera Aproximación, itBSC=BSC



BSC: Balance ScoreCard



Dirección

Objetivos Estratégicos

Rutinas, sin plazo

Hitos, con plazo

itBSC: Perspectiva Financiera

- Objetivos:
  - Control de Costes del Negocio
  - Economía en la provisión de IT
  - Retorno de la inversión en infraestructura
  - Administración de contratos de IT
- Procesos ITIL:
  - Financial Management of IT Services
  - Service Level Management

itBSC: Perspectiva Cliente

- Objetivos:
  - Disponibilidad de servicios de IT
  - Performance en servicios de IT
  - Confiabilidad en la infraestructura
  - Servicios medibles en dinero
  - Soporte de usuarios de IT
- Procesos ITIL:
  - Service Level Management
  - Availability Management
  - IT Serv. Continuity Management
  - Financial Management
  - Incident Management y Service Desk

itBSC: Proceso Interno

- Objetivos:
  - Staff bien definido, IT Knowledge Management
  - Eficiencia en la provisión del servicio
  - Capacidad de Procesamiento
  - Seguridad
  - Contabilidad de provisión de IT
- Procesos ITIL:
  - Problem Management
  - Service Desk
  - Service Level Management

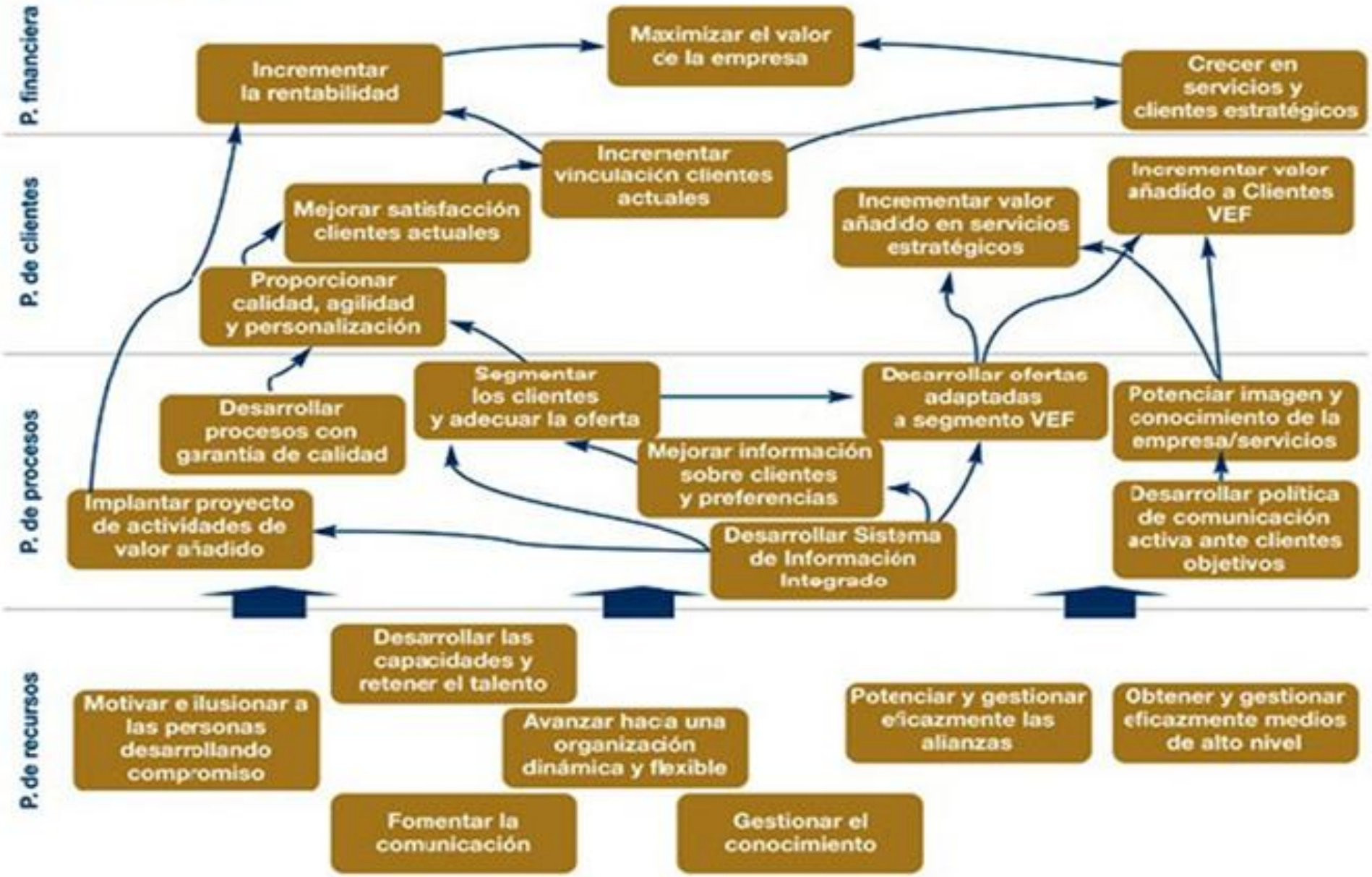
itBSC: Aprendizaje y Crecimiento

- Objetivos:
  - Flexibilidad en la infraestructura de IT
  - Controlar los cambios de servicio e infraestructuras
  - Adaptabilidad a la demanda cambiante en el negocio
  - Comunicación y transferencia de conocimiento
  - Productividad del negocio en relación con los costos
- Procesos ITIL:
  - Service Level Management
  - Capacity Management
  - Change Management
  - Financial Mgt. of IT Services

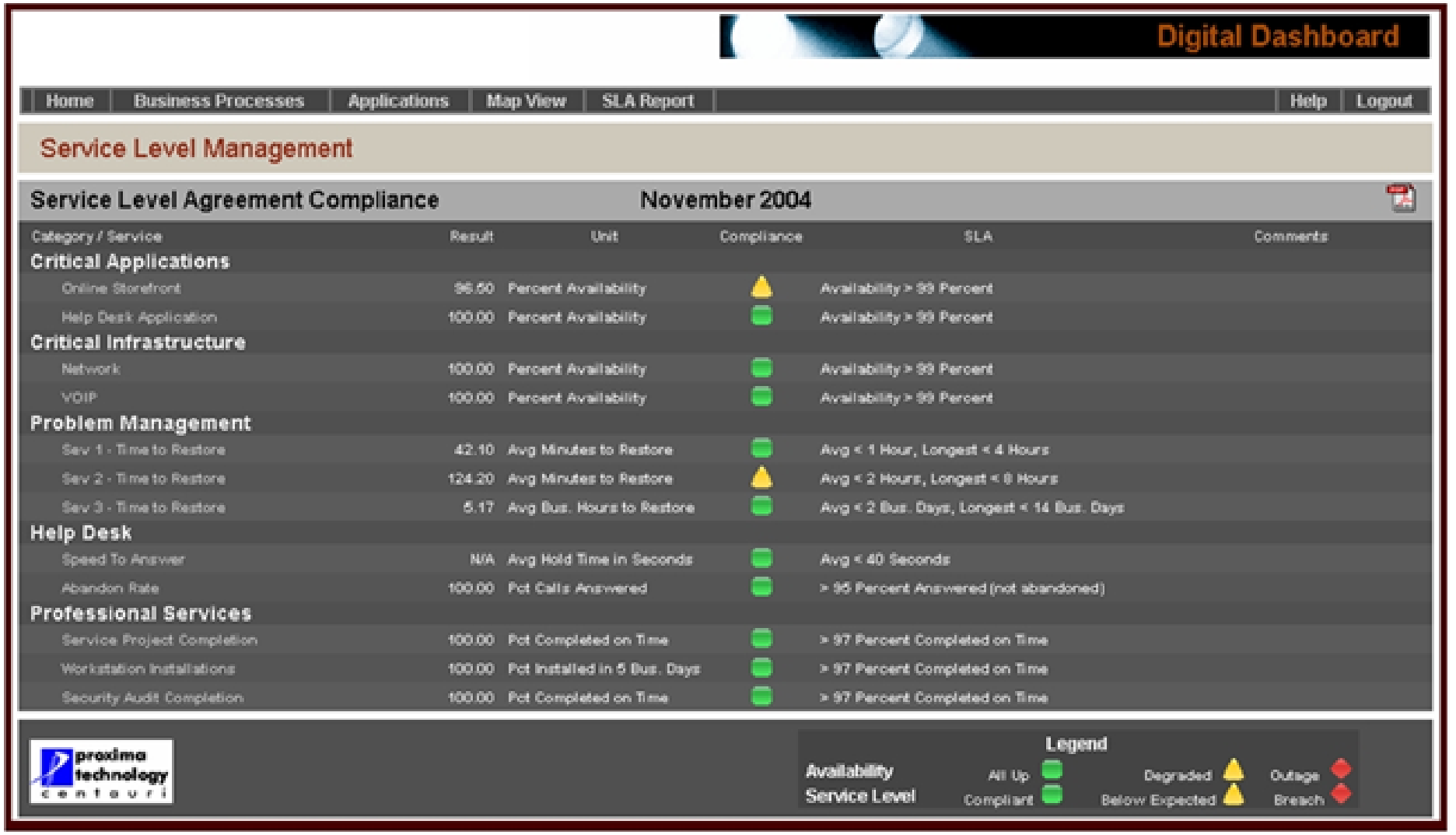
ItBSC: Balance ScoreCard para TI

- Debe ser capaz de cubrir:
  - > Garantizar la "orientación a negocio", los planes y actividades de TI alineadas con los objetivos y necesidades del negocio.
  - > Canalizar el esfuerzo de la organización de TI según sus objetivos.
  - > Establecer medidas claras de medición de la efectividad y eficiencia de TI.
  - > Estimular y sostener los niveles de rendimiento de TI.
  - > Alcanzar y balancear los objetivos de los diferentes stakeholders.

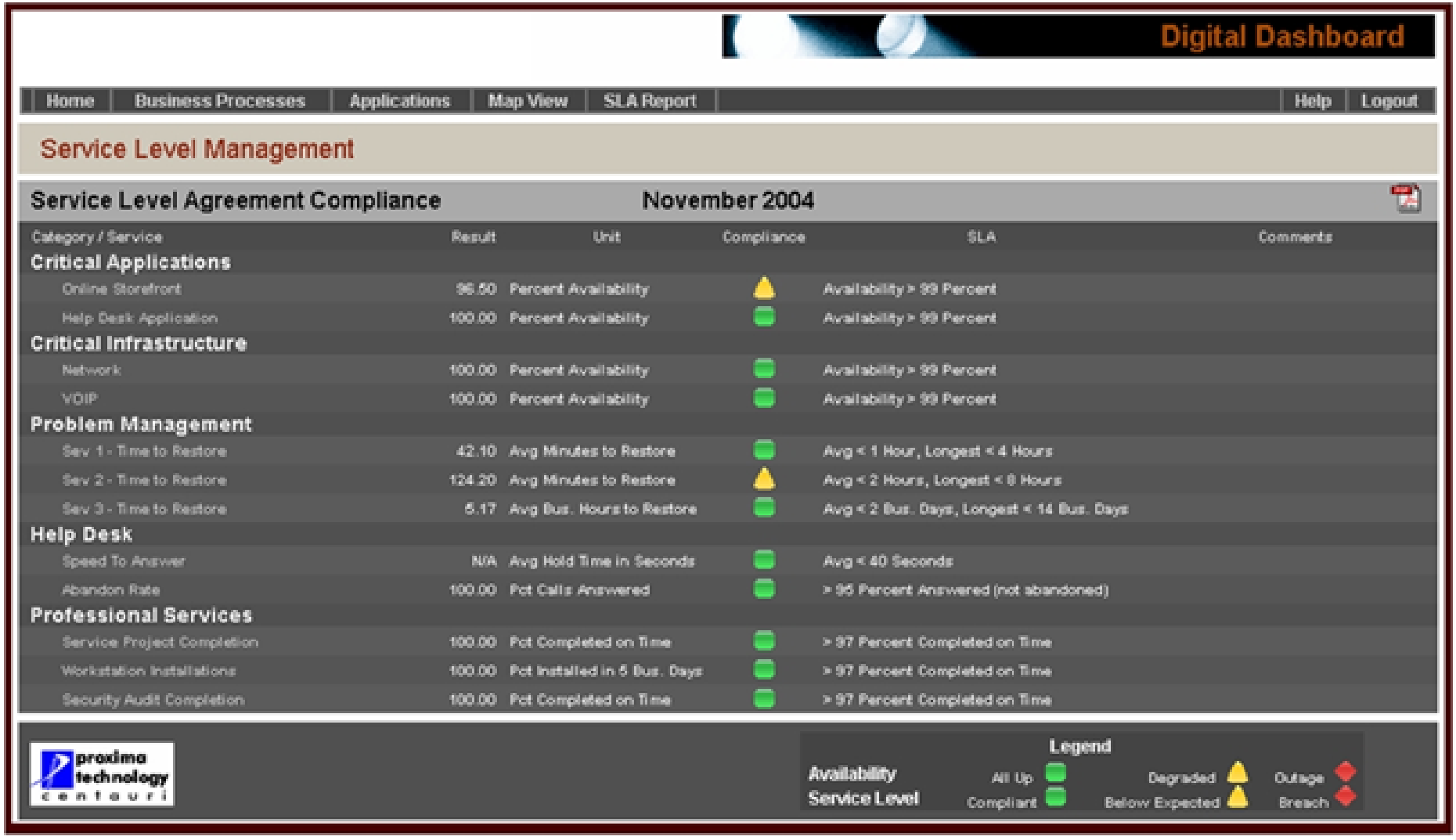
Mapa estratégico



Automatización



Automatización



Digital Dashboard

Home | Business Processes | Applications | Map View | SLA Report | Help | Logout

Service Level Management

Service Level Agreement Compliance — November 2004

Category / Service	Result	Unit	Compliance	SLA	Comments
Critical Applications					
Online Storefront	96.50	Percent Availability	▲	Availability > 99 Percent	
Help Desk Application	100.00	Percent Availability	■	Availability > 99 Percent	
Critical Infrastructure					
Network	100.00	Percent Availability	■	Availability > 99 Percent	
VOIP	100.00	Percent Availability	■	Availability > 99 Percent	
Problem Management					
Sev 1 - Time to Restore	42.10	Avg Minutes to Restore	■	Avg < 1 Hour, Longest < 4 Hours	
Sev 2 - Time to Restore	124.20	Avg Minutes to Restore	▲	Avg < 2 Hours, Longest < 8 Hours	
Sev 3 - Time to Restore	5.17	Avg Bus. Hours to Restore	■	Avg < 2 Bus. Days, Longest < 14 Bus. Days	
Help Desk					
Speed To Answer	N/A	Avg Hold Time in Seconds	■	Avg < 40 Seconds	
Abandon Rate	100.00	Pct Calls Answered	■	> 95 Percent Answered (not abandoned)	
Professional Services					
Service Project Completion	100.00	Pct Completed on Time	■	> 97 Percent Completed on Time	
Workstation Installations	100.00	Pct Installed in 5 Bus. Days	■	> 97 Percent Completed on Time	
Security Audit Completion	100.00	Pct Completed on Time	■	> 97 Percent Completed on Time	

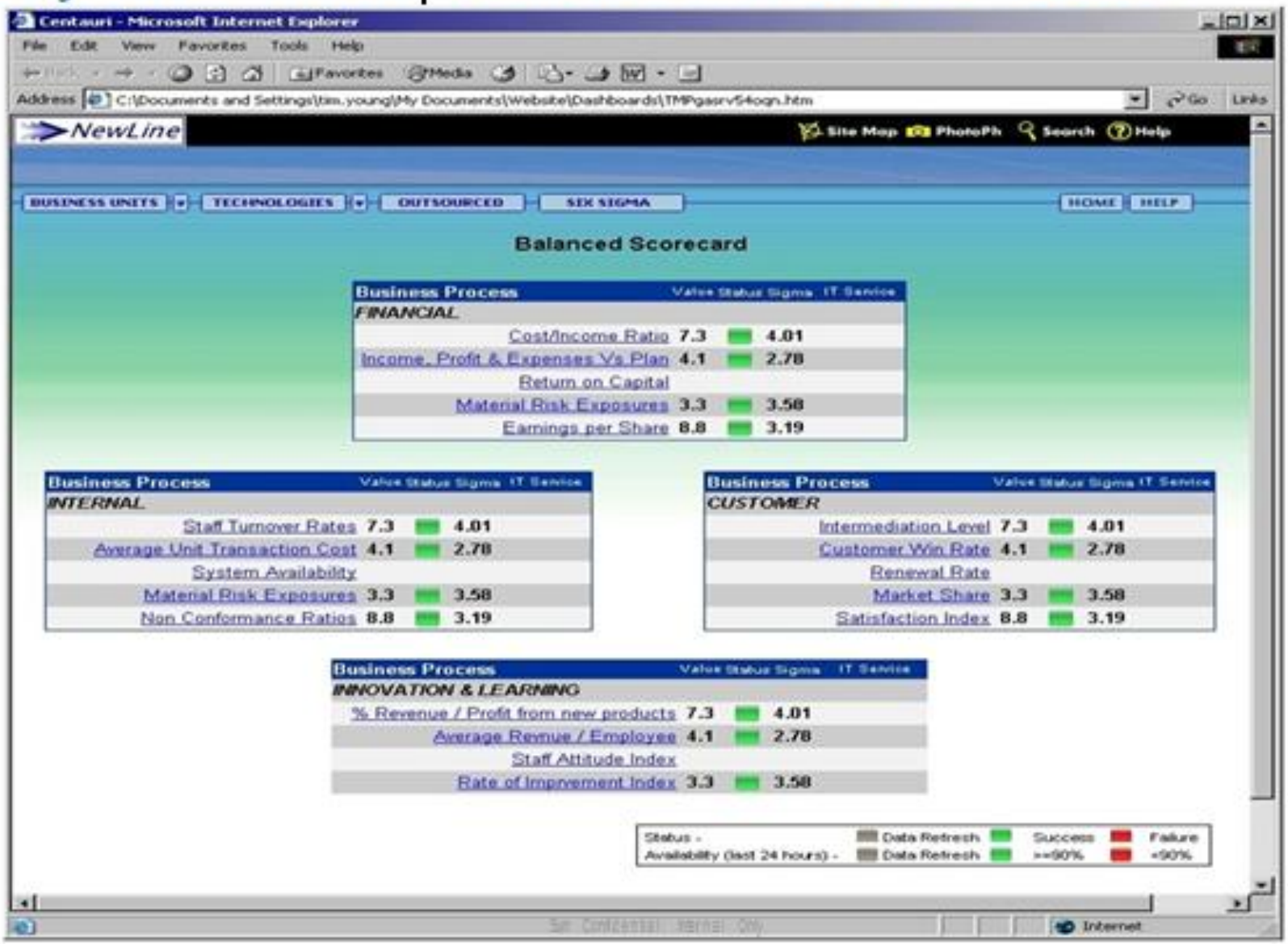
proxima technology centauri

Legend

Availability	All Up ■	Degraded ▲	Outage ◆
Service Level	Compliant ■	Below Expected ▲	Breach ◆

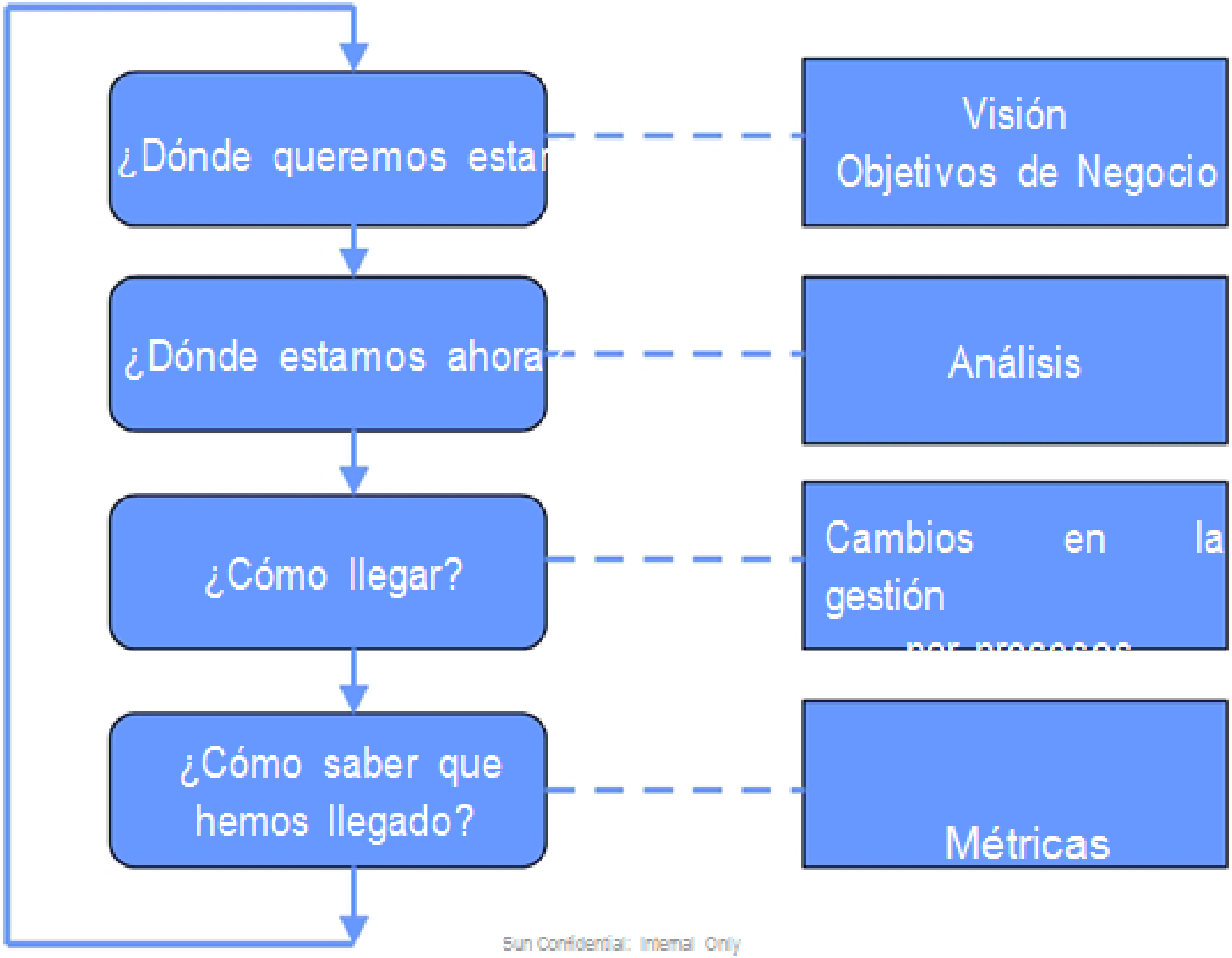
Automatización

Objetivo final: Balanced Score Card

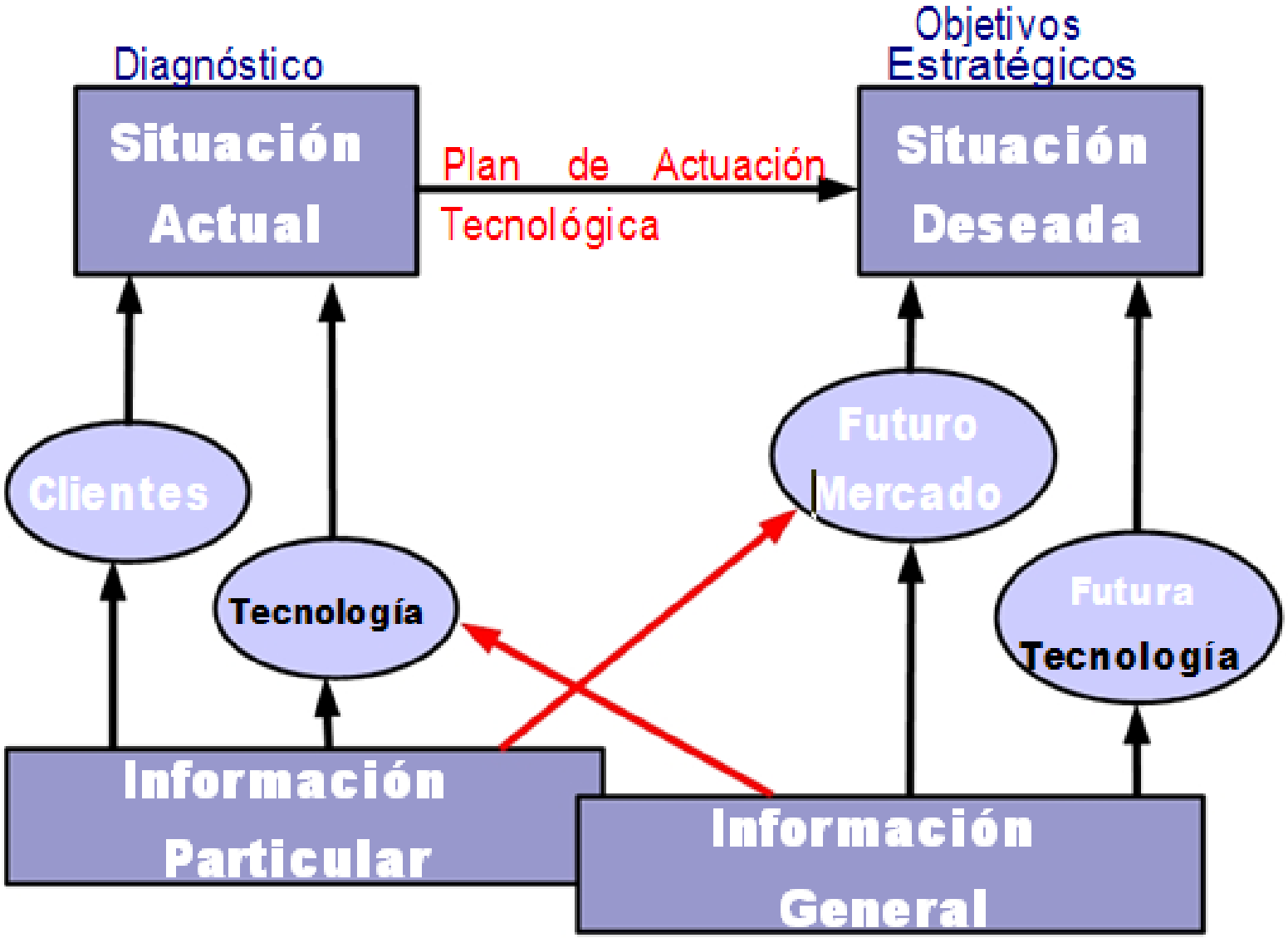


Plan de Adopción

Alineamiento con el Negocio



Alineamiento con el Negocio



Roadmap Servicios ITIL